Advanced Sciences and Technologies for Security Applications

Anthony J. Masys *Editor*

Exploring the Security Landscape: Non-Traditional Security Challenges

Springer

Advanced Sciences and Technologies for Security Applications

The series Advanced Sciences and Technologies for Security Applications focuses on research monographs in the areas of

- Recognition and identification (including optical imaging, biometrics, authentication, verification, and smart surveillance systems)
- Biological and chemical threat detection (including biosensors, aerosols, materials detection and forensics),

and

- Secure information systems (including encryption, and optical and photonic systems).

The series is intended to give an overview at the highest research level at the frontier of research in the physical sciences.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at http://www.springer.com/series/5540

Anthony J. Masys
Editor

Exploring the Security Landscape: Non-Traditional Security Challenges

Springer

Editor
Anthony J. Masys
University of Leicester
Leicester
UK

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-319-27913-8 ISBN 978-3-319-27914-5 (eBook)
DOI 10.1007/978-3-319-27914-5

Library of Congress Control Number: 2015958842

Printed on acid-free paper

This Springer imprint is published by SpringerNature
The registered company is Springer International Publishing AG Switzerland

Contents

Introduction

Anthony J. Masys

Today's security landscape has been described as transnational in nature. In light of this, the security studies domain has seen a deepening and broadening in response to the changing landscape. In addition to the issues pertaining to the traditional security concerns of threat, force and state actors, non-traditional security issues have emerged. For example, matters pertaining to AIDS, SARS and Ebola pose health threats but also have significant national security implications. Transnational crime has become global in scale and is no longer exclusive to certain geographical areas. The increased transnational flow of people, goods, money and information as products of 'globalization' has also changed the security landscape in terms of the 'globalization' of transnational crime. With the advent of cyberspace and the inherent interdependencies, a condition of 'hyper-risks' (Helbing 2013) has emerged thereby contributing to security challenges. Health security, economic security, food security and energy security are interrelated concepts that characterize the security landscape as complex. Actions and interventions associated with this complex problem space can have highly unpredictable and unintended consequences.

1 Security Challenges

As part of the Springer book series: Advanced Sciences and Technologies for Security Applications, this edited volume: Exploring the Security Landscape: Non-traditional Security Challenges, focuses on examining various perspectives associated with security that does not fall into what is normally considered traditional security concerns.

A.J. Masys (✉)
University of Leicester, Leicester, UK
e-mail: anthony.masys@gmail.com

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_1

This book comprises 15 chapters from leading researchers engaged in examining emerging national and global security concerns.

2 Content

Miloš Jovanović et al. in their chapter 'Non-traditional Transnational Security Challenges in Serbian, British and Dutch Security Discourses: A Cross Country Comparison' ask the questions: What are a country's traditional and non-traditional security challenges? How are these security challenges being discussed and by whom, and how does this discussion relate to a country's neighbours and a pan-European perspective? What is the relevance of human security, ethics and human rights to these security issues? Questions like these are often addressed in security policies, which are required to be both legitimate and effective and should address the concerns (including ethical) of different stakeholders across the European Union. Yet to date an overview of these concerns does not exist. Research conducted within the FP7 funded project "The Evolving Concept of Security (EvoCS)—A critical evaluation across four dimensions"[1] fills this gap with a cross-disciplinary methodology using empirical methods to measure subjective security perceptions. This chapter presents an overview of these perceptions across the Netherlands, Serbia and the UK and in doing so provides a description of the project's methodology.

Christian O. Fjäder in his chapter 'National Security in a Hyper-Connected World' explores the opportunities and threats this hyper-connectivity presents to national security, specifically from an economic security point of view. How can national critical societal functions and infrastructures be secured against transnational and extra-sovereign dependencies that extend beyond the mandate of sovereign states? Moreover, how can a nation secure its external "lifelines" without violating the sovereignty of states these reside in or pass through? In the theoretical level these questions relate to the sovereign state's autonomy of action in economics and national security in a system that increasingly functions on transnational and extraterritorial logic.

Ioannis Chapsos in his chapter 'Is Maritime Security a Traditional Security Challenge?' discusses contemporary maritime security and examines the extent of its (non-)traditional nature in the context of international security. Based on the existing literature and adopted strategies, the chapter highlights that there is no internationally accepted definition. Arguably, maritime security's concept depends on the perspective of the 'end user' and it broadens as far as the relevant

[1] The partners of this multi-national project are the Hague Centre for Strategic Studies HCSS (The Netherlands), Loughborough University (UK), Procon (Bulgaria), Istituto Affari Internazionali IAI (Italy), Università Cattolica del Sacro Cuore UCSC (Italy), Tecnalia (Spain), Polski Instytut Spraw Miedzynarodowych PISM (Poland), and Scuola Superiore Sant'Anna di Studi Universitari e di Perfezionamento SSSUP (Italy). It is coordinated by Fraunhofer INT (Germany).

stakeholders get involved. Still, contemporary maritime security is directly linked and interdependent with human security and development. The combination of human insecurity's non-traditional nature and the increasing involvement of non-state actors in projecting maritime insecurities, results in its differentiation from the traditional, interstate security challenges.

Marie-Jo Medina in her chapter, 'Pandemic Influenza Planning for the Mental Health Security of Survivors of Mass Deaths' recognizes that Influenza A pandemics have been documented to occur at 10- to 50-year intervals—an average of three events per century, dating back from the 16th century. Each recorded pandemic has resulted in an increase in annual mortality rates in the infected population, with mass deaths in one pandemic wave equaling fatalities sustained over six months of an epidemic season. This chapter aims to rectify the oversight in pandemic preparedness plans by presenting a compendium of guidelines and recommendations by international health organisations, pandemic fatality experts, and experienced mass death management professionals. Its objective is to have available a mass fatality framework to complement the WHO Pandemic Influenza Preparedness and Response guideline 2009, from which individual national pandemic preparedness plans are based. It is written in a format that incorporates WHO's emphasis on finding the ethical balance between human rights and successful plan implementation; the assimilation of national pandemic plans with existing national emergency measures; and the 'whole group' system of engaging individuals, families, localities, and business establishments in the process. This chapter is also written such that it can be made applicable to analogous infectious disease outbreaks like SARS and Ebola, as well as comparable mass fatality events.

Paul Canfield in his chapter 'An evaluation of the Police Response to Gang-related Violence and Future Security Threats' shows that over the past decade Bermuda has experienced a dramatic increase in gang violence. The United Nations Office on Drugs and Crime's Global Study on Murder showed that Bermuda's murder rate had increased from 3.1 per 100,000 people in 2003 to 12.5 in 2011 (Strangeways 2010). While the increased prevalence of gangs is not something that is unique to Bermuda (Bullock and Tilley 2002; Battin-Pearson et al. 1998), the sharp increase was a cause of great concern within the local community, the police and politicians (Parliamentary Joint Select Committee 2011). The reason for this may be that Bermuda's economy relies largely on tourism (Central Intelligence Agency 2013) and international business, especially reinsurance, which increased its presence on the island since the terrorist attacks in New York and Washington on the 11th of September 2001. Any increase of gang violence in an otherwise peaceful and low crime country may deter future investment in the island (The Washington Post 2006). This research primarily seeks to outline the development of Bermuda's gang culture and how the Bermuda Police Service (BPS) responded to the gang violence. It has been suggested that gang-related crime is essentially a social problem and not just an undertaking for the police, but the community as a whole (Muncie 1999). Socio-economic factors may have also influenced the development of gang crime in Bermuda, but this research focuses on the situational crime prevention strategies that the BPS adopted and whether these strategies have helped to reduce gang violence and whether these techniques may be considered suitable in preventing a rise in terrorism.

Christian Leuprecht in his chapter 'The Demographic horizon of the emerging security environment' peruses the causes, consequences and implications of changes in the supply and demand side of consequences of demographic change as a non-traditional transnational challenge in the emerging security problem space. Demography is the study of population structure and change as a result of interaction effects among fertility, mortality and immigration. Political demography is the study of how change in the size, distribution, and composition of population affects both politics and government. It examines communal relations, political behaviour and social institutions as a process of change in demographic trends. This chapter in particular surveys distributive effects of resources and political power as a result of changing urban and rural, religious, regional, ethnic, elite, and cohort population subgroups, and their impact on domestic, regional and global security environments.

Tyler Valdron in his chapter 'Economic Security: An emerging security issue' argues that corporate actors most certainly have a stake in large economic nodes and so their decisions and incentive structures within the larger system should not be ignored. Insurance-industry corporate actors play a particularly relevant role when it comes to economic security because if we evaluate the incentives of this specific set of decision makers, we quickly see that they have a great vested interest in evaluating the economic security of a node, or system of nodes, and investing accordingly. Where they show concern by upping insurance costs or otherwise asking for better security in an area or class of assets, there is with good probability a very real threat to economic security worthy of further investigation by state actors. Understanding these incentives towards action when it comes to corporate actors can then logically be very informative to state actors who wish to maintain effective economic security.

Tie Xu and Anthony J. Masys in their chapter 'Critical Infrastructure vulnerabilities: embracing a network mindset' argues that in the past decade, unprecedented technological advancements, rapid institutional changes and trans-boundary dependencies have changed the landscape of infrastructure systems. Critical infrastructure has now evolved into highly interconnected and interdependent networks of socio-technical systems in which different technological layers are interoperating crossing borders within the environmental, social and organizational context that drive their design, operations and development (Masys 2014a, b). Understanding the nature of system interdependencies and emerging vulnerabilities can play an essential role in managing and/or reducing the probabilities and consequences of cascading failures in interdependent systems. In this light, the overall objective of this chapter is to address the knowledge gap existing in the dominant risk and disaster management theories by challenging and improving our networked mental model in order to better understand the interdependency-induced vulnerability pertaining to critical infrastructures thereby developing effective protection measures and enabling organizational resilience (Masys 2012). For policy makers, infrastructure owners/operators and researchers as target audience, this chapter will identify emerging challenges to the traditional security thinking in this field and suggest alternative approaches to risk assessment and vulnerability analysis.

Tie Xu and Shereen Nassar in their chapter 'Supply Chain Information Security: emerging challenges in the telecommunications industry' argue that given the ramifications of widespread RFID implementation in contemporary supply chain management, there is a need for awareness of emerging security threats and effective self-protection mechanisms for system failures and attacks. The aim of this chapter is to identify the emerging information security challenges pertaining to RFID applications in the telecommunications industry. For policy makers and telecoms operators as target audience, this chapter will present a conceptual framework for approaching risk management activities in regards to Auto-ID/RFID applications with comprehensive and contemporary understanding about information assets, ecosystem threats, and vulnerabilities embedded in their extended supply chains.

Anthony J. Masys in his chapter 'Disrupting terrorist and criminal networks: Crimescript analysis through DODAF applications' shows that the complexity of the current threat landscape associated with terrorism and criminal networks continues to be a top national and global security agenda item. With heightened awareness and concern regarding the proliferation and expansion of ISIL and connections to homegrown violent extremism, understanding the network structure and functional perspectives is a key enabler to supporting counter terrorism disruption strategies. Challenges associated with understanding these 'dark networks' stems both from contextualizing the information (plagued by uncertainty and ambiguity) and from the multiplex nature of the actors whereby they can share more than one type of relation. In this exploratory work, Counter-Terrorism Architectural Frameworks (CTAF) is introduced as an application of the Department of Defense Architectural Frameworks (DODAF) to support 'opening the blackbox' of terrorist activities to identify terrorist network vulnerabilities and to develop disruption strategies. The multiple views afforded by the application of DODAF provides a more comprehensive picture to support decision making and can highlight the complex organizational dynamics that are not readily observable through Social Network Analysis (SNA) alone. In this chapter the methodology is explained and applied to an analysis of the Lashkar-e-Taiba (LeT) terrorist network (Subrahmanian et al. 2013) and the Noordin Top terrorist network (Roberts and Everton 2011).

David Skillcorn and Christian Leuprecht in their chapter 'Beyond the Castle Model of Cyber-risk and cyber-security' explains why the defence in depth: higher, better layers of walls that approach for secure computing is as outmoded for cybersecurity today as it became for physical security centuries ago. Three forces are undermining the castle model as a practical security solution. First, organizations themselves tear down their walls and make their gateways more porous because it pays off in terms of better agility and responsiveness—they can do more, faster and better. Second, technological developments increasingly destroy walls from the outside as computation becomes cheaper for attackers, and the implementation of virtual walls and gateways becomes more complex, and so contains more vulnerabilities to be exploited by the clever and unscrupulous. Third, changes in the way humans and technology interact, exemplified (but not limited to) the Millennial generation, blur and dissolve the concepts of inside and outside, so that distinctions become invisible, or even unwanted, and boundaries become annoyances to be circumvented. A new approach to cybersecurity is needed: Organizations and individuals need to get used to operating in compromised environments. This chapter's conclusion operationalizes this strategy in terms of a paradigm shift away from a Castle Model and towards a more nuanced form of computation and data assurance.

Anna Brinkmann and Karolin Bauer in their chapter 'Food Security as Critical Infrastructure: the importance of safeguarding the food supply for civil security' show how vulnerabilities in critical infrastructures can cause significant hardships to the affected population during crises and large scale disasters like Hurricane Sandy in 2012 or the nuclear catastrophic event Fukushima in 2011. Referring to this, critical infrastructures include "primary physical structures, technical facilities and systems whose disruption, failure or destruction have a serious impact on the functioning of society, the economy or the state within a natural hazard induced disaster context" (United Nations 2011:6). As a component of critical infrastructures, Food and especially the Food Supply is a significant part of the services for the public and fundamental for an effective Civil Security System. In this chapter primary definitions regarding Food as a critical infrastructure are depicted as the meaning of safeguarding the food supply in case of crisis or disaster situations emerges as critically important.

Ken Wewa-Wekesa in his chapter 'The role of Social Network Sites in security risks and crises: The information warfare of terrorism' addresses a key concern regarding terrorism, radicalization and violent extremism. Social Network Sites (SNS) have in recent years received significant universal attention in the way they have changed lives socially, politically and economically through distinct components that enable people from all over the world to connect instantly. This work analyses the aggressive nature in which terrorists quickly adapt to these SNS vis-à-vis governments' approach to risk communication and situational crisis communication using the same media. It additionally examines literature on the publics' cumulative behaviour regarding the use of SNS in the context of terror attacks and the terrorists' use of the same media to coordinate their operations in recruiting people to join their organisations, planning and execution of terror attacks. To achieve that, this chapter investigates the online cumulative behaviour which has been witnessed recently (e.g. during the Westgate Mall attack by Al-Shabaab in Nairobi, Kenya in 2013) and the terrorists taking advantage of these platforms (e.g. the Islamic State of Iraq and Syria [ISIS]) to stimulate crises of national security.

Anthony J. Masys in his chapter 'Manufactured Risk, complexity and non-traditional security: from world risk society to a networked risk model' reflects upon Beck's (1992, 2009) claim that we inhabit a Risk Society. With the advent of global climate change, extreme weather, transnational crime, NATECH's (natural disaster triggered technological disasters), and terrorism, Beck's notion of 'manufactured risks resonates with the non-traditional security domain that includes:

economic security, energy security, environmental security, health security and food security. This is all about complexity framing. Beck (1992) risk discourse regarding manufactured risks and effects that are both temporally and spatially displaced resonates with the complexity notion of nonlinearity. Hence the inherent interdependencies and interconnectivity that characterizes the risk space leads to a network model. The notion of hyper-risks (Helbing 2013; Masys et al. 2014) captures well the interconnectivity and complexity of the security threats. The complexity lens thereby becomes prominent in examining security. A networked risk model emerges as a construct that links Becks risk discourse to non-traditional security challenges.

Together the chapters highlight the broadening and deepening of security perspectives and challenges associated with the non-traditional security domain.

References

Battin-Pearson SR, Thornberry TP, Hawkins JD, Krohn MD (1998) Gang membership, delinquent peers, and delinquent behavior. Department of Justice, Office of Juvenile Justice and Delinquency Prevention Bulletin. Youth Gang Series. Washington, DC

Beck U (1992) Risk society: towards a new modernity. Sage, London

Beck U (2009) World at risk. Polity Press, Cambridge

Bullock K, Tilley N (2002) Shootings, gangs and violent incidents in Manchester: developing a crime reduction strategy. Crime reduction research series paper, vol 13. Home Office, London

Central Intelligence Agency (2013) The world factbook: Bermuda. The Central Intelligence Agency. https://www.cia.gov/library/publications/the-world-factbook/geos/bd.html. Accessed 9 Sept 2013

Helbing D (2013) Globally networked risks and how to respond. Nature 497:51–59

Masys AJ (2012) Black swans to grey swans—revealing the uncertainty. Int J Disaster Prev Manage 21(3):320–335

Masys AJ (2014a) Critical infrastructure and vulnerability: a relational analysis through actor network theory. In: Masys AJ (ed) Networks and network analysis for defence and security. Springer, Berlin

Masys AJ (2014b) Dealing with complexity: thinking about networks and the comprehensive approach. In: Masys AJ (ed) networks and network analysis for defense and security. Springe, Berlin

Masys AJ, Ray-Bennett N, Shiroshita H, Jackson P (2014) High impact/low frequency extreme events: enabling reflection and resilience in a hyper-connected world. In: 4th international conference on building resilience, procedia economics and finance, vol 18, 8–11 Sept 2014. Salford Quays, UK, pp 772–779

Muncie J (1999) Deconstructing criminology. Crim Justice Matters 34:4–5

Parliamentary Joint Select Committee (2011) Joint select on the causes of violent crime and gun violence in Bermuda: a parliamentary joint select committee publication under Part 1 V of the parliamentary act 1957, July 2011. Available from http://www.parliament.bm/uploadedFiles/Content/Home/Report%20on%20Violent%20Crime%20and%20Gun%20Violence%20in%20Bermuda.pdf. Accessed 11 Nov 2012

Roberts N, Everton SF (2011) Strategies for combating dark networks. J Soc Struct 12(2). http://www.cmu.edu/joss/content/articles/volume12//RobertsEverton.pdf

Strangeways S (2010) Bermuda's per capita murder rate was more than five times London's Rate in 2009, *RoyalGazette.com*. The Royal Gazette, 9 Jan. 2010. Available from http://www.royalgazette.com/article/20100109/NEWS/301099993. Accessed 13 Sept 2013

Subrahmanian VS, Mannes A, Siliva A, Shakarian J, Dickerson JP (2013) Computational analysis of terrorist groups: Lashkar-e-Taiba. Springer, Berlin

The Washington Post (2006) Gang violence jolts formerly quiet Bermuda; tourist Getaway grapples with string of shootings highbeam research. The Washington Post, 6 Aug 2006. Available from http://www.highbeam.com/doc/1P2-139686.html. Accessed 3 Aug 2013

UNISDR—United Nations National Strategy for Disaster Reduction (eds.) (2011) National strategy for disaster reduction. Themes and issues in disaster risk reduction, [Online] Available: http://www.preventionweb.net/files/23647_themesandissuesindisasterriskreduct.pdf. [Accessed 01.07.2015].

Non-traditional Transnational Security Challenges in Serbian, British and Dutch Security Discourses: A Cross-Country Comparison

Miloš Jovanović, Tim Sweijs, Ksenia Chmutina, Francesca Vietti, Roberto Franzini Tibaldeo, Joachim Burbiel, Lee Bosher and Andrew Dainty

Abstract What are a country's traditional and non-traditional security challenges? How are these being discussed and by whom? What is the relevance of security, ethics and human rights to these issues? Questions like these are often addressed in security policies. Yet to date an overview of these concerns does not exist. Research conducted within the project EvoCS fills this gap. This chapter presents an overview of these perceptions across the Netherlands, Serbia and the UK and provides a description of the methodology. The majority of the salient security challenges in all three countries are also prominent in the EU policy discourse. In conclusion, the three analysed countries are surprisingly similar to each other, considering the many differences between them. From a European point of view, this might be seen as an opportunity since future European Security Strategies can better address shared security problems of both EU and (possible future) non-EU members.

Keywords Concepts of security · Policy making · Cross-country comparison · Security dimensions

M. Jovanović (✉) · J. Burbiel
Fraunhofer INT, Euskirchen, Germany
e-mail: Milos.Jovanovic@int.fraunhofer.de

T. Sweijs
The Hague Center for Strategic Studies, The Hague, The Netherlands

K. Chmutina · L. Bosher · A. Dainty
Loughborough University, Loughborough, UK

F. Vietti
Scuola Superiore Sant' Anna di Studi Universitari e di Perfezionamento, Pisa, Italy

R. Franzini Tibaldeo
Université Catholique de Louvain, Louvain-la-Neuve, Belgium

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_2

1 Introduction

What are a country’s traditional and non-traditional security challenges? How are these security challenges being discussed and by whom, and how does this discussion relate to a country’s neighbours and a pan-European perspective? What is the relevance of human security, ethics and human rights to these security issues? Questions like these are often addressed in security policies, which are required to be both legitimate and effective and should address the concerns (including ethical) of different stakeholders across the European Union. Yet to date an overview of these concerns does not exist. Research conducted within the FP7 funded project “The Evolving Concept of Security (EvoCS)—A critical evaluation across four dimensions”[1] fills this gap with a cross-disciplinary methodology using empirical methods to measure subjective security perceptions. This chapter presents an overview of these perceptions across the Netherlands, Serbia and the UK and in doing so provides a description of the project’s methodology. The present three were chosen in order to facilitate a comparison between two countries which, being in the same region, at first glance seem rather similar (the UK and Netherlands, both in North-western Europe) and an example from South-eastern Europe (Serbia), which due to its historical context may seem very different.

The project comprises four regional case studies which were conducted applying an analytical framework (that will be described in Sect. 2). The four case studies dealt with four model regions in Europe (the “core countries” which are studied in depth are given in brackets, see also Fig. 1):

- West-Mediterranean EU (Italy, Malta, Spain)
- Eastern EU Border (Poland, Hungary, Lithuania)
- North-Western EU (United Kingdom, Netherlands, France)
- South-Eastern Europe (Serbia, Bulgaria, Turkey)

The preliminary results of the national case studies for the Netherlands, Serbia and the UK are described in Sect. 3, while Sect. 4 discusses the transnational aspects of the security challenges found in the national case studies.[2]

[1] The partners of this multi-national project are the Hague Centre for Strategic Studies HCSS (The Netherlands), Loughborough University (UK), Procon (Bulgaria), Istituto Affari Internazionali IAI (Italy), Università Cattolica del Sacro Cuore UCSC (Italy), Tecnalia (Spain), Polski Instytut Spraw Miedzynarodowych PISM (Poland), and Scuola Superiore Sant’Anna di Studi Universitari e di Perfezionamento SSSUP (Italy). It is coordinated by Fraunhofer INT (Germany).

[2] The results of EvoCS are accessible to European political decision makers and security end-users, for example to support the work on future European security strategies by comparing the various national security concepts and the similarities and differences they have and which regional and pan-European conclusions can be drawn from them. Additionally, the results of EvoCS will be used to inform future research projects in Horizon 2020.

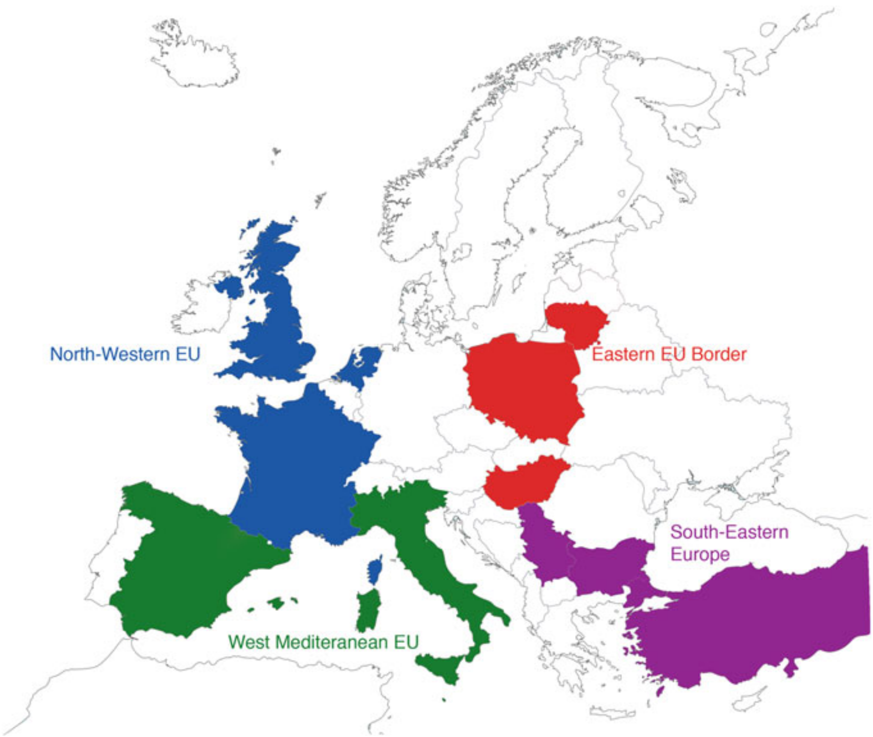


Fig. 1 The four EvoCS regions. The colour-coded countries are analysed in the case studies

2 The EvoCS Analytical Framework

Initially, an analytical framework was developed by four teams consisting of multiple country experts to assess national and regional variation in security concepts in twelve countries across Europe. The key objective was to offer a multifaceted overview of key security concerns amongst various country level constituencies in the European Union (EU). Alongside this endeavour a model has been created which periodically gauges changes in these security concerns based on a combination of quantitative and qualitative analyses. Transparency and replicability of the methods were therefore indispensable elements of the analytical framework. Another central element is the notion of a security concept as it exists in the eye of the beholder. Security is seen as a socially constructed phenomenon (see for example Buzan et al. 1998). A concept of security consists of five dimensions[3]: the *core values* which refer to the different aspects of life that actors seek to secure

[3] Originally, the EvoCS project envisioned only four dimensions. In the course of the project, this number changed to five.

including physical safety and security, territorial integrity and security, environmental and ecological security, social stability and security, cultural identity and security, political stability and security, economic prosperity and security and information and cyber security [4]; the types of *security challenges* that affect these core values which can be either risks, threats or hazards [5]; the *levels* at which security needs to be protected which may include the local, subnational, international, transnational and global level; the *actors* that are involved including—but not limited to—national or local government, the private sector, civil society or the individual citizen; and the *ethical and human rights issues* which manifest themselves in this process. Different beholders prioritise different core values and perceive different security challenges; they prefer these to be addressed by different actors at different levels, and consider different ethical and human rights issues to be a problem. In order to assess these differences empirically, the research process was divided in two stages (see Fig. 2).

In the first stage, country teams assessed currently prevailing security concepts in their respective countries across six principal security discourses: government, parliament, academia, media, the private sector and the NGO sector.[6] These discourses were selected because they reflect important contributions to societal debates about concepts of security from different angles. For each discourse in each country, a similar set of documents was retrieved based on a set of predefined criteria and a set of detailed retrieval instructions. The documents were then manually coded; this process relied on a uniform coding scheme in order to elicit various concepts of security. The results were then recorded in a centrally managed online data repository to which all country team researchers had access. Both the set of criteria and instructions as well as the coding scheme were the product of multiple online and offline discussions between the researchers. The outcome of

[4] In identifying these dimensions and taxonomies we looked at a wide range of academic and policy documents. In the latter category we examined official security policy documents of France, Great Britain, Poland and the Netherlands. We have also drawn extensively from the European Trends and Threats in Society (ETTIS) project which analysed security discourses in academic sources and official security policy documents of European countries. See ETTIS consortium (2012).

[5] Risks, threats and hazards are three related but distinct concepts. A threat is a "potentially damaging physical event, phenomenon or activity of an intentional/malicious character", in contrast to a hazard, which is non-directional in nature. Neither a threat nor a hazard involves the element of chance of the threat or hazard materialising involved. Risk is the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences". Risk thus not only looks at likelihood but also takes into account both the vulnerability of the target of the risk. The relationship could be described as follows: *Possibility of threat/hazard occurring* * (*threat/hazard* * *vulnerability of target*) = *Risk*. In popular security discourses, they are sometimes used interchangeably, which is why we decided to first record them as security challenges. See European Commission (2011b) and DHS Risk Lexicon (2010).

[6] As our objective is to assess national perceptions of security, international governmental organizations (IGOs) do not appear on this list. IGOs certainly affect national concepts of security, but only indirectly through one of the sources on this list.

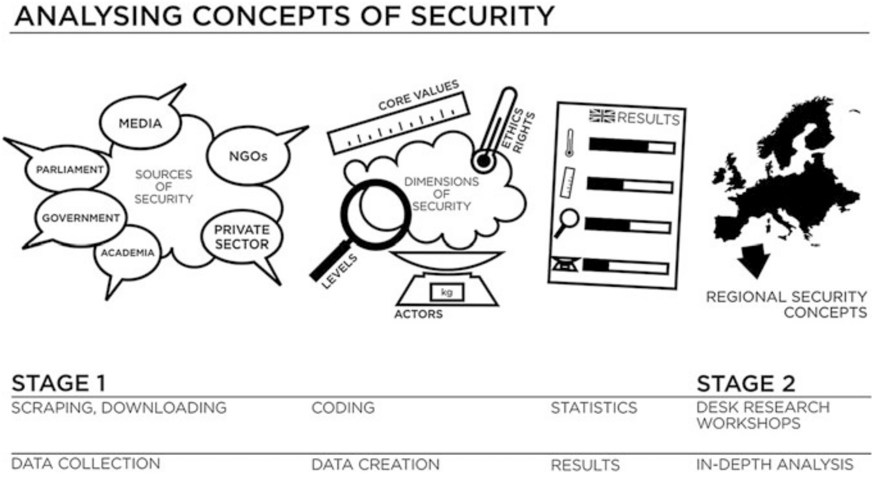


Fig. 2 The analytical framework

these discussions was subsequently codified in the 'Assessing Evolving Concepts of Security: Coding Handbook' (see Sweijs et al. 2015), which was employed by country team researchers during the entire coding process. In order to promote inter coder reliability, country teams first coded a small batch of documents, discussed the results and calibrated their approach in case of disagreement. Inter coder reliability in the North Western Europe team was 87 % for a set of 20 documents selected from the different discourses. During the process, any ambiguities or uncertainties were flagged and discussed, and kept a written record of in an online document in order to improve the accuracy of the coding and maintain consistency.[7] In total, over 3425 documents across 12 countries have been analysed.[8]

Stage one of the research process thus yielded a semi-quantified overview of prevailing security concepts across and within different countries. Stage two served to both corroborate and substantiate the findings yielded in stage one. In stage two the findings were then further analysed in desk research and a series of workshops which were held around Europe in early 2015. Here the principal purpose has been to get a more granular understanding based on in-depth qualitative analysis of the findings unearthed in stage one. For each country, further analysis was undertaken of the core values that are perceived to be affected by particular security challenges, of the levels of action which are singled out and the actors which are involved, as well as the ethical issues which are at stake. Salient differences between discourses within and across countries were then highlighted and further explored in order to

[7] To this purpose two internal working documents *Coding Better* and *Coding Changes* were shared in the online repository and regularly updated. These documents are available upon request.

[8] Our raw data are available upon request and interested researchers are cordially invited to make use of what we consider to be a treasure trove of data.

provide a better understanding of thinking about security in different countries. Also in stage two, the evolution of country concepts of security over the past decade was described qualitatively to get a better grip on the recent historical context in which it emerged.

For the purposes of this book chapter, we have used this dual track approach drawing on quantitative and qualitative analysis to identify the salience of non-traditional security challenges in security discourses in the Netherlands, Serbia and the United Kingdom.[9] Each section first succinctly describes some of the key findings for security discourses in these three countries (and their transnational aspects) and proceeds by identifying key non-traditional security challenges, the core values they affect, the actors and the levels of appropriate action and the ethical and human rights issues that are singled out across the three countries.

2.1 The Human Rights and Ethical Aspects of the Analytical Framework

Ethics and human rights are often perceived as incompatible with or unrelated to security (see for instance Balzacq and Carrera 2006; Weinblum 2010), as if they were mutually exclusive or the pursuit of security could be achieved without respecting fundamental rights and ethical principles. However, ethics and security are not irreconcilable precisely thanks to the recognition and codification of human rights at regional and international level in the course of the past seventy years.

Human rights are values and legal guarantees grounded on the recognition that "all human beings are born free and equal in dignity and rights" (United Nations General Assembly 1948). Human rights are universal, inalienable, indivisible, and interrelated (United Nations General Assembly 1993). Besides being codified (de jure), they must be safeguarded and enjoyed (de facto). In this regard, States have to respect, protect and fulfil fundamental rights in their jurisdictions.[10] Moreover, ethics and human rights are inextricably linked: the recognition of human rights is closely related to coeval trends in philosophy, according to which ethical reflection ought to provide principles viz. general guides of action, whose aim is to "provide a standard of relevance or 'reasonableness'" (Carlberg 2008) for human conduct. As

[9] The authors of this chapter were the lead researchers on the three country case studies. The three countries share substantial similarities as well as substantial differences in terms of their size, history, security culture and geographic location. As such this concise assessment of prevailing key security concepts illustrate what a cross country comparisons of security concepts across the Europe Union can yield. Interested readers are invited to visit the EvoCS website at http://evocs-project.eu/.

[10] The obligation to respect entails that States refrain from interfering with the enjoyment of human rights; the obligation to protect requires States to protect both single individuals and groups against human rights abuses and the obligation to fulfil implies that States take positive action to facilitate the enjoyment of basic human rights. See for instance Freeman (2011).

a result, ethics provides a heuristic tool (or a critical and reflective lens) (Schön 1983) enabling us to understand how we can fulfil a meaningful life and a properly 'human' existence (See Ricoeur 1992; Sen 1979; Nussbaum and Sen 1993; Nussbaum 2001, 2011; Hursthouse 2012). In this perspective, ethics is—just like human rights—based on human dignity (see Kant 1785; Oviedo convention, 1997, art. 1), as a notion endowed with 'normative' relevance. This means, that human dignity is something that *ought* to be pragmatically fostered in compliance with specific ethical principles and operational guidelines.[11]

The recognition of human rights has contributed to acknowledging that secure states could be inhabited by insecure people and that global security needed to be conceived to include the protection of people against those challenges threatening their survival and well-being in their daily lives (see United Nations 1992; Commission on Global Governance 2005). This allowed shaping the notion of security as human-centred and multi-dimensional. Human security entails freedom from want, freedom from fear and freedom to live in dignity. It implies protecting people from critical (severe) and pervasive (widespread) threats and situations (see United Nations Development Program 1994; Commission on Human Security 2003). Such a paradigm calls for responses which need to be people-centred, comprehensive, context-specific and prevention-oriented, aimed at strengthening the protection and empowerment of all people and all communities (United Nations Trust Fund for Human Security 2009). In this regard, as underlined by the European Agenda on Security "security and human rights are not conflicting aims but consistent and complementary policy objectives" (European Commission 2015).[12] Security and human rights are mutually reinforcing: on the one hand, a secure environment is conducive to the enjoyment of human rights; on the other hand, the respect, protection and fulfilment of fundamental rights contributes to the maintenance of peace as well as to enhancing security in peoples' daily lives. In particular, the recognition of the human dimension in the security discourse has profound implications, as it reconsiders security in terms of 'security of whom?' 'security from what?,' and 'security by what means?' (Tadjbakhsh and Chenoy 2007).

Thus, human rights and ethics provide a 'normative' framework and an overall perspective thanks to which it is possible to understand, interpret and eventually assess specific events as well as overall trends related to security. Since security is inextricably related to ethics and human rights, EvoCS investigated the extent to

[11] Indeed, the philosophical reflection of the last centuries encouraged an understanding of the ethical dimension through the lens of concepts, such as universality, equality, individuality, human flourishing, which were practically operationalized into corresponding 'normative' claims and guidelines. See among others: Rawls 1971; Bobbio 1996; Nussbaum 2011; Reis Monteiro 2014; Loretoni 2014; Wolters 2015.

[12] This implies that "All security measures must comply with the principles of necessity, proportionality and legality, with appropriate safeguards to ensure accountability and judicial redress" (European Commission 2015).

which the security discourse, both at national level and in the four regions, considered ethical and human rights principles.[13]

3 Preliminary Results from the Case Studies

3.1 The Netherlands

Concepts of security abound in the Netherlands. The Dutch government codified its interpretation of national security in its 2007 'Strategy National Security' (SNS) [*Strategie Nationale Veiligheid*] (Ministerie van Veiligheid en Justitie, Strategie Nationale Veiligheid 2007). Here it defined national security to consist of five vital interests: (1) territorial security, (2) physical security, (3) economic security, (4) environmental security, and (5) social and political stability. National security is only affected when one of these five vital interests is threatened to such an extent that there is potential societal disruption. The SNS has been reflective of a broader evolution in various Dutch security discourses in which (national) security is understood not only with reference to traditional security risks but also in relation to an array of challenges within a multifaceted concept of security. In this concept, not only robust capabilities for security and defence forces, but also communal trust and societal resilience are acknowledged to be essential pillars of security across different discourses. The government continues to be considered—both by itself but also by other actors—as a pivotal player in the protection of security, as we found in our analysis of hundreds of documents within the EvoCS research project.[14] But increasingly, the private sector and civil society writ large are seen not only as consumers but also as producers of security (Oosterveld et al. 2015). Sharing the burden of responsibility for security at the domestic level is actively encouraged by the government—and not only in the cyber domain—even if this is not always

[13] In order to make ethics and human rights operational, a list of relevant human rights and ethical principles has been provided to the researchers, namely: rights/human rights/fundamental rights, ethic* (ethics, ethical), dignity, non-discrimination, human security, autonomy, privacy/integrity, equality, liberty/freedom (of assembly, of association), transparen* (transparency, transparent), universal* (universality), equality/diversity (as a value). No hierarchy exists among these principles, since "all human rights are universal, indivisible and interdependent and interrelated" (see United Nations General Assembly 1993). The coding process produced an outcome in terms of the following three codes: 'main topic', if ethical and human rights principles are the primary focus of the piece of evidence; 'mentioned', if they are present; 'absent', if there is no consideration of ethical and human rights principles. Subsequently, a pondered assessment allowed investigation of the reasons behind the outcome of the coding process.

[14] This is based on a manual coding of the most recent national security strategies issued by the government, transcripts of 100 Parliamentary debates about security, a sample of NGO, academic and corporate publications on security, as well as 200 articles from two leading newspapers (*De Volkskrant* and *De Telegraaf*) in the period 31 Oct 2013–1 November 2014. For more information see Sweijs et al. 2015

matched by the allocation of adequate resources. Self-reliance (‘*Zelfredzaamheid*’) and resilience meanwhile have transformed from buzz words into mainstream concepts in both popular and political security discourses. Yet, the expectations of citizens and corporations with regards to what the state can and will do for them in this field, are sometimes pointed out to be excessively large (Dutch Court of Audit Algemene 2014, 22). When it comes to the locus of responsibility for security provision, the key trend for the Netherlands can be characterised as evolving from an accelerated push towards the privatisation of responsibility for security in the 1990s and early 2000s, to bringing the state back in as a response to terrorist attacks abroad and political assassinations in 2002 and 2004 at home. In the 2010s, there is an incremental but still nascent transition to a whole-of-society approach in which various actors acknowledge that they will have to play an active part, even if there is disagreement about the appropriate scope, reach and division of these responsibilities.

Across different Dutch security discourses, the four most salient core values identified in our coding for the EvoCS project are physical safety and security, economic prosperity and security, territorial integrity and social stability and security. The tragic downing of flight MH17 over Ukraine on 17 July 2014—in which close to 200 Dutch citizens lost their lives—and the ongoing conflicts in the Middle East and North Africa, have shifted the focus from internal to external security challenges, both for government, the private sector and civil society. Whereas previously profits and principles were dominant themes in various Dutch security discourses, peace has once again returned to the forefront.[15] In government and media security discourses, there has been a discursive shift of attention towards challenges to physical safety and security but also to territorial integrity, which have complemented rather than substituted those challenges affecting economic prosperity and human rights.[16]

In our analysis for the EvoCS research project, we found a wide array of security challenges that are identified, with their salience varying significantly across different sources. Both media and government give ample attention to physical safety and security and social stability. Government and corporate actors worry about

[15] Here we’re paraphrasing an oft used characterization of Dutch foreign policy to consist of a mix of Peace, Profits and Principles as coined by Joris Voorhoeve in his 1979 book that carried the same title.

[16] As codified in the Dutch Constitution one of the core tasks of the armed forces is to uphold international law. Article 97 of the Dutch Constitution reads: ‘There shall be armed forces for the defence and protection of the interests of the Kingdom, and in order to maintain and promote the international legal order.’ (http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrndb9f5vzi, last accessed 13 May 2015) Rather than being considered a relic of times past, official justifications for the deployment of armed forces always involve arguments about how it contributes to the strengthening of human rights. See Sweijs (2009) at http://www.hcss.nl/reports/dutch-military-intervention-decision-making-revisited-getting-a-constitutional-grip-on-21st-century-wars/28/.

economic prosperity and security with especially the latter singling out cyber security challenges as a source of concern. Key security challenges include, but are not limited to:

- The Russia-Ukraine conflict (physical safety and security and economic prosperity and security)
- Transnational religious violence (physical safety and security and social stability and security)
- Cyber vulnerabilities (economic prosperity and security)
- Natural hazards (physical security and economic prosperity and security)

These EvoCS findings are also corroborated by a representative bi-annual survey called the *Ipsos Risk and Crisis Survey* [*Risico—En Crisis Barometer*] commissioned by the Office of the Coordinator of Terrorism and Security (Dutch acronym: NCTV) to map security concerns of Dutch citizens (NCTV 2014). In late 2014—the latest edition at the time of writing—security concerns about potential spill-over effects from the transnational conflict in the Middle East topped the list of concerns, followed by concerns over challenges to economic prosperity. The participants in the survey were also presented with a prefabricated list of security challenges and asked to express the depth of their concern. Both interestingly and characteristically, ten out of thirteen security challenges on this list—which was compiled under the aegis of the NCTV—could be classified as non-traditional security challenges. The challenges included, but were not limited to, an economic crisis, epidemics, cyberattacks, accidents with hazardous substances, disturbances of vital (electricity, gas water or ICT) infrastructures and flooding (NCTV 2014). Concerns about spill-over effects of an international crisis affecting the Netherlands topped the list.

For a variety of economic, cultural and geographical reasons, the intertwining of external and internal security challenges as well as the non-traditional nature of many of them, is both explicitly and implicitly recognised in the Netherlands. The official 2013 international security strategy titled “A Secure Netherlands in a Secure World” as well as its 2014 update make this point before mentioning a variety of non-traditional challenges affecting Dutch security interests, including—but certainly not limited to—the transnational nature of religious violence and organised crime, the changing composition of the world economy, the global implications of climate change, and water and resources scarcity (Ministerie van Buitenlandse Zaken 2013, 2014). Our analysis for the EvoCS project shows that in Dutch security discourses, the appropriate level of action to deal with these challenges is not only identified to be national, local, and international, but that also the global and the transnational levels are relatively often mentioned.

In addition to recognising the external and internal security nexus, the relationship between traditional and non-traditional security challenges is increasingly emphasised, in wider societal discussions as well as in some of the documents analysed in the context of the EvoCS project. Most poignantly this is illustrated by a series of earthquakes in the Northern part of the Netherlands which set off a discussion about how to deal with the relationship between safety, energy security, prosperity, physical security, and ethics and human rights. Following years of minor earthquakes in the Northern part of the Netherlands, in 2015 the Dutch government finally acknowledged that the quakes were the result of gas drilling in the area. This has not only led to a curtailing of some of the drilling activities, but it has also prompted an ongoing debate about how this will affect Dutch energy dependencies internationally, specifically vis-å-vis Russia.[17] In the debate about the future of gas drilling, various security concerns receive ample attention: shielding Dutch citizens from man-induced natural disasters, safeguarding economic security, reducing energy dependency, protecting the physical security of Dutch citizens travelling on international air lines of communication, and identifying and bringing to justice those responsible for the events of 17 July 2014. Whether the Dutch will opt for peace, for profits or for principles remains to be seen for now; but it is clear that the relationship across these different domains—as well as the tradeoffs between them—is well understood.

In sum, our analysis finds that non-traditional and transnational aspects of security challenges are well represented across various Dutch security discourses, both official and non-official ones. In addition to recognizing the internal and external security nexus, the intricate relationship between traditional and non-traditional security challenges is increasingly acknowledged as a quintessential characteristic of the contemporary security landscape.

3.2 Serbia

The Republic of Serbia published its national security strategy back in 2009 (see Government of Serbia 2009). Comparing this with the results of the Serbian coding exercise represents a challenge, since the coding mostly provided a snapshot of the end of 2013 and 2014. However, since national security strategies normally have a very long-term perspective, the comparison led to some interesting leads regarding security, its perception and discourse in Serbia. The coding showed that both long-term and short-term security challenges were part of the security discourse. In this context short-term challenges are those which are characteristic for the years 2013/2014 but were not prominently present roughly before or after that period (one example being lengthy discussions on a new Serbian law on traffic security which was passed in 2014). Long-term challenges, on the other hand, are those which have been part of the security discourse for a much longer period. Some of them were also mentioned in 2013 and 2014, some were not.

[17] Relations between the Netherlands and Russia had already significantly deterioriated in the wake of Russia's *Blitzanschluss* of the Crimea. But they reached an all time low following the downing of flight MH17, which—it is widely asserted in various societal discourses, although the Dutch government reserves judgment for now—may have happened by accident, but was executed with some form of Russian involvement.

The most prominent core values discussed in Serbia in those years were physical safety and security, followed by economic prosperity and security and social stability and security. Physical safety and security is a core value that comes up very often in the national case studies. One probable reason for this is that it is a much broader category than, for example, information and cyber security. The security challenges that lie behind the core values are varied, some of them mentioned in the national security strategy some not (e.g. the proliferation of weapons of mass destruction is one risk mentioned in the national security strategy but was not discussed in the Serbian context in 2013/2014). Generally, one can cluster the Serbian security challenges into two categories, both including short-term and long-term security challenges:

1. "Traditional" security challenges like corruption, natural hazards and man-made disasters, organized crime, discrimination against ethnic and religious minorities and hooliganism. Some of these are transnational in their nature (for example organized crime).
2. "Non-traditional" security challenges (as understood in the present book) some of which are "unique" to Serbia, at least in the context of the Southeast European region. The conflict with Kosovo, the very high number of refugees in Serbia and Serbia's geopolitical situation are part of this category as well as information and cyber challenges.

Since this book chapter focusses on the non-traditional and transnational security challenges, we will take a closer look at the contents of the second category. Some of the challenges of category 1, however, are also transnational in their nature and will be mentioned where reasonable:

- **Conflict with Kosovo**: This security challenge includes both judicial aspects (the question of the legitimacy of the declaration of independence) and the situation of the Serbian minority in Kosovo, which is very often discussed as part of the physical safety and security core value. The latter is quite interesting, because originally, this challenge was probably part of the core value on territorial integrity and security. It seems that seven years after the declaration of independence the security has shifted from the judicial aspects (which are still important, but less so than before) to the practical daily life of citizens living in Kosovo.
- **Effects of the Yugoslav civil war**: One of the aftereffects of the Yugoslav civil wars, which mostly took place in the 1990s, is a very high number of Serb refugees in Serbia who fled from the wars in Croatia, Bosnia and Kosovo.
- **National and religious extremism**: This security challenge is explicitly mentioned in the national security strategy. Apart from the aspects of this challenge that are tied to the first two mentioned in this list, a new one has been shown in the coding exercise: Serbian citizens (and/or Kosovar citizens) that travel to Iraq and Syria to join the Islamic State (IS) and later on return to their country. This is a challenge that Serbia shares with its European neighbours, even though the problem is much more prevalent in Kosovo than in Serbia proper.

- **Geopolitical situation**: Serbia has declared military neutrality, tries to become part of the European Union and traditionally has strong ties to Russia. This unique mix is discussed in the context of security.
- **Organized crime**: This security challenge is one of the most often mentioned in the security discourse. Drug and human trafficking, money laundering and smuggling all are crimes that have a transnational character, even though the security challenge as such is a rather "traditional" one.
- **Cyber and information challenges**: While these security challenges are normally considered to be non-traditional, the Serbian discourse on them is rather national. Spying on citizens and the Serbian president, hacker attacks on ATM machines and video surveillance of traffic are some examples for what is being discussed.
- **Natural hazards**: This is another example of a traditional security challenge that has a transnational character. Once a natural hazard takes place (like the floods in northern Serbia in May 2014), it becomes part of the security discourse but it also gradually fades away again. In case of some of these natural hazards, the transnational character becomes apparent when the natural hazard is of a magnitude that hits more than just one country. In this context, the national security strategy also mentions global warming as one of the central risks to Serbia. However, it is not mentioned very often in the security discourse.

Summing up Serbia's non-traditional security challenges (and the traditional ones that have a transnational character) and adding to it the fact that most of the security discourse takes place on a national level, one can say that Serbia shares such security challenges as natural hazards, cyber and information challenges and organized crime with many of its direct and wider European neighbours. Others, like the ones dealing with the effects of the Yugoslav civil war are shared with direct neighbours like Croatia or Bosnia & Herzegovina and are typical for the Southeast European region. Finally, security challenges like the situation in Kosovo are unique to Serbia and are only seldom transnational (if one excludes the question of whether Kosovo's declaration of independence was legitimate or not), e.g. when one deals with citizens that leave the country to fight for IS. From an ethical and human rights point of view, Serbia's security discourse often deals with discrimination against religious, ethnic or the Serbian lesbian, gay, bisexual and transgender (LGBT) community. This is relevant in view of the recent past and it highlights the need to protect and promote minorities' rights in order to build an inclusive society.

During the regional workshop on Southeast Europe, one participant remarked that from his point of view Serbia sees itself "surrounded by enemies" (Jovanovic et al. 2014). Comparing this to the overview of the security challenges one has to wonder whether this is still the case. Similar to other countries, Serbia's traditional security challenges are becoming more and more transnational in their nature while the number of non-traditional security challenges is also growing. However, Serbia's national security strategy includes most, if not all, of the challenges which were found during the coding exercise. This speaks for the strategy but also for a closer examination as to whether the mentioned security challenges have actually been addressed.

3.3 United Kingdom (UK)

The term “national security”—whilst widely used—is not specifically defined by the UK Government. It has been the policy of successive Governments and the practice of Parliament not to define the term, in order to retain the flexibility necessary to ensure that the use of the term can adapt to changing circumstances (MI5 2014). As a matter of Government policy, the term “national security” is taken to refer to the security and well-being of the UK as a whole. ‘Security policy’ had remained as an abstract concept till the New Labour Government came into power in 1997, and was mainly based on foreign and defence policy (Clarke 1998). The overarching principles of security have changed with the Conservative and Liberal-Democrat coalition Government coming to power in 2010, and are now focusing on ‘all-encompassing’ national security that addressed security ‘in the round’ incorporating linked areas of policy including counter-terrorism, international aid and diplomacy, border and cyber security, and homeland defence (as opposed to a security strategy that was primarily focused on defence and Armed Forces) (Almandras et al. 2010).

The EvoCS coding exercise has demonstrated that the most prominent security core values in the UK are physical safety and security, economic prosperity and security, and environmental and ecological security. The most prominent security challenges identified using the EvoCS coding methodology align with the UK security challenges emphasised in the National Security Strategy (NSS) (HM Government 2010):

- **Terrorism** is listed as the highest priority risk with the principal security challenge being international terrorism, however different types of attacks are expected (including ‘lone wolves’, residual terrorism groups etc.).
- **Cyber-attacks** are also the highest priority risk which government, the private sector and citizens are prone to, with the risk emanating from both hostile states and individual criminals. Cyberspace is integral to the UK economy, thus providing various opportunities as well as threats.
- **Energy and food supply** appear to be lower risks; they are defined as ‘*disruption to oil or gas supplies to the UK, or price instability, as a result of war, accident, major political upheaval or deliberate manipulation of supply by producers*’ and ‘*short to medium term disruption to international supplies of resources (e.g. food, minerals) essential to the UK*’ respectively (HM Government 2010).
- **Climate change** is not included in the tiers of risks but is considered a security issue (which is aligned with EC security concerns): “*Our security is vulnerable to the effects of climate change and its impacts on food and water*”, concluding that “*the physical effects of climate change are likely to become increasingly significant as a ‘risk multiplier’, exacerbating existing tensions around the world*” (HM Government 2010).

- Climate change goes hand in hand with another security challenge—**natural hazards**. Flooding, for instance, is the highest priority risk due to the potentially high impacts and disruptions such events can cause. Whilst the NSS only focuses on floods, the 'National Risk Register' also lists storms and gales, drought, severe effusive (gas-rich) volcanic eruptions abroad, low temperatures and heavy snow, heatwaves, and severe wildfires (Cabinet Office 2013).

The comparison of security challenges noticed in the NSS and in the popular discourse demonstrates that security challenges in the latter tend to be long-term; they have been acknowledged as such for a number of years, and there is no indication that they will be removed from the agenda in the nearest future. Radicalisation (i.e. 'radicalised Britons') is not mentioned in the NSS but has become prominent very recently (from 2014) and has captured the newspaper headlines as well as being prominent in political statements. Cyber security is becoming increasingly important, largely due to the use of cloud computing. Whilst the Cyber Security Programme is ending in 2016, it is most probable that new frameworks will be developed as cyber threats impact upon the economic development of the UK and will do so more in the future, with the Internet playing a prominent role in business development.

Climate change and natural hazards will also remain prominent but to a different extent. Depending on the priorities of the next UK Government, climate change may receive less attention as its impacts are not deemed to be immediate or obvious. In addition, climate change is hard to securitise because it is understood very differently by different government departments (with the environmental side of it being predominant). Natural hazards on the other hand are—although reactively—increasingly being viewed as relevant to the security agenda, particularly after the floods in winter 2013. Whilst UK energy and food supply systems are believed to be relatively resilient, there are a number of risks (e.g. severe weather, terrorism, technical failures, industrial action) that can be mitigated but cannot be avoided entirely. Energy supply has also received a lot of attention in 2014 due to the deterioration of the political relationship with Russia, when a specific question on whether UK supply will be able to meet the UK demand in the future was posed. In 2013 the UK's net energy import dependency climbed to 47 %, the highest level since 1975, and energy exports reached their lowest level since 1980. In the same year, coal was the source of 36 % of UK electricity generation, gas contributed 27 %, nuclear 19 %, renewables 15 %, and others contributed 3 % (DECC 2014). Given the fall in domestic energy production, the rise in the UK's energy import dependence and particular reliance on Russia for coal imports, it is vital to find ways to secure the supplies of energy. Food supply is similarly a long-term security challenge: the current strategy is already discussing the threats that may affect the UK food supply in 2030. This security challenge is closely linked to the threats posed by climate change, natural hazards and energy supply.

Whilst human rights and ethical issues are mentioned with regards to all of the threats, they are hardly discussed in relation to cyber-attacks. This is surprising as with the discourse on data loss and communications interceptions, cyber-attack could be seen as the most ethically relevant one.[18] This could be consistent with the securitization approach according to which in presence of non-traditional security challenges of highest priority risk by hostile states or criminals, greater focus is put on the alert rather than on a reflection regarding the ethical and human rights implications.

All sources raise human rights and ethical issues, however different publications find different threats as a matter of human and ethical concern. For instance, newspapers purely focus on terrorism, whereas parliament publications mention human rights and ethical issues across all of the threats. Overall, human rights and ethical issues are not perceived to be a salient part of security discourse in the UK.

When comparing the national political debates and popular discourses, a number of UK security features become apparent:

- ‘Hard’ (which mainly include physical) security challenges are often prioritised over other security challenges: as such general events that don’t affect the wider population directly (e.g. the murder of Lee Rigby) can trigger a determined political discourse that receives more attention than the events that directly influence citizens (e.g. impacts of natural hazards).
- Security is a ‘reactive’ process (events disrupting trends): Security appears to be about knee-jerk reactions, but ideally should be about being able to accommodate events within consistent policy frameworks.
- Globalisation of security: Events that occur outside of the UK—and Europe—can have direct impacts upon the security situation in the UK. Globalisation has a direct impact on security thinking.
- The phenomena of ‘widening security’: Non-security events have become securitised, because in doing so it can make it possible to quickly mobilise resources. For instance in securitising ‘climate change’ it could make it more ‘justifiable’ for policy makers to mobile resources to deal with the impacts of a changing climate.

This overview of the most prominent security challenges demonstrates that the UK is gradually moving from the ‘traditional’ security challenges towards a more inclusive and broader security framework, which is motivated by the increasing complexity of inter-sectoral issues. With a large number of actors involved in, and affected by, security challenges at different levels, it is becoming more and more difficult to clearly identify security dimensions (Chmutina et al. 2015). The political, governance, economic, physical, social, environmental and other security core values are interconnected and form a complex system of inter- and intra-dependent networks that mutually support each other.

[18] This finding may be a result of a methodological limitation, as human rights and ethical issues were only coded when explicitly stated.

4 Discussion and Conclusions

The three case studies presented in this chapter are but a part of a total of 12, which were compiled in the EvoCS project.[19] Overall, the results of these case studies demonstrate that the existing threats will remain salient in the near future and addressing them requires thinking about the global context that can become a driver of the negative influences upon national and local security. Security has been re-framed from national interest to a more local human security-oriented discourse, but at the same time national, even regional interests are becoming important again. Some security challenges are either unique to a country (e.g. the conflict with Kosovo) or to a region (e.g. the effects of the Yugoslav civil war). The same is true for some challenges like the protection of the physical security of Dutch citizens travelling on international air lines (e.g. flight MH17), which has had a major influence on the Dutch security discourse and cannot be found in other EU countries.

On the other hand, some softer security challenges, which have only recently been securitised (e.g. environmental and ecological security issues such as climate change) are much more prominently discussed in the North-western countries. Here they are discussed not only as a threat multiplier that is already putting greater pressure on the stability of fragile societies, but also as a significant challenge to the physical security and economic prosperity of these littoral states itself due to rising sea levels (opposed to the landlocked Serbia which perceives less immediate danger).

The three countries, however, have much in common, from the point of view of security challenges and their public discourse. Both the UK and Serbia intensively discuss the core values of physical safety and security and economic prosperity and security and so does the Netherlands. The former might be due to the broad definition of this core value.

In all three countries, non-traditional security challenges are becoming more and more important and are discussed accordingly. These non-traditional security challenges such as religious violence, organised crime and cyber-attacks, natural hazards and climate change are also similar in all three countries, and are gaining prominence in the security discourse. Also, the national security strategies in all three countries address most, if not all, of these non-traditional security challenges and there exists a shift towards "transnationalisation" of the security challenges.

One of the most interesting findings of this coding exercise is the realisation that whilst theoretically—and on the European level[20]—human rights are suggested to play an important role, this issue is not prominent in most of the security discourses. Whilst the majority of the sources acknowledge human rights and ethics related issues, these are hardly ever discussed as the main topic; instead they seem to be

[19] For the detailed project deliverables, please visit http://www.evocs-project.eu/deliverables.

[20] A special section in the new European Agenda on Security (2015) is given to addressing human rights, which are the key for the security strategy.

used as an add-on. The main reason for this is that the present-day security discourse highlights a dialectical tension between opposing trends: notwithstanding its theoretical reframing into a human security-oriented perspective (which entails the relevance of human rights and ethics, along with the support granted by transnational institutions, like the EU), in the political and mass-media discourse the notion of security seems still to rely on a conventional, basically pragmatic, competitive and State-centred conduct coping with challenges threatening States. It is noteworthy to mention that, at least according to their national security strategies (Government of Serbia 2009; HM Government 2010; Ministerie van Buitenlandse Zaken 2013), in UK and the Netherlands this second trend appears to be stronger than in Serbia. In the latter case, it is interesting to note that the actor that addresses ethical and human rights issues by far the most often is civil society. Similarly, in relation to the number of sources coded, Serbian NGO sources were the ones that most often referred to ethical and human rights issues.

The majority of the salient security challenges in all three countries are also prominent in the EU policy discourse, and are becoming more so as the new EU Strategy is being implemented. The overall findings refer not only to the threats of terrorism and cyber-crime, but to other salient threats listed in Sect. 4.1: the EU has implemented an Energy Security Strategy (EC 2014); it runs a Food security thematic programme aimed at internal and external food supplies (EC 2011c); and has developed an extensive EU Adaptation package with the EU Strategy to Climate Change at its heart (EC 2013). However some differences were also found. For instance, as expected, the EU level documents promote cooperation among the member states as well as with the third country partners, however the specific countries that should, for instance, take a lead on addressing a particular challenge are rarely named. On the contrary, the case study countries—whilst mentioning cooperation, focus largely on their own efforts, capacities and capabilities in addressing various challenges.

In conclusion, the three analysed countries are surprisingly similar to each other, considering the many historical and political differences between them. Of course, there are some typical national and regional challenges in Serbia, but the similarities to the North-western countries seem to outweigh the differences. From a European point of view, this might be seen as an opportunity since future European Security Strategies can better address shared security problems of both EU and (possible future) non-EU members.

References

Algemene R (2014) Zicht Overheden op Beschermen Burgers en Bedrijven. Nederland

Almandras S et al (2010) UK defence and security policy: a new approach? The house of commons. Commons library research paper. UK

Balzacq T, Carrera S (eds) (2006) Security versus freedom? A challenge for Europe's future. Ashgate, Farnham

Beck U (1992) Risk society: towards a new modernity. Sage, London

Bobbio N (1996) The age of rights. Polity Press, Cambridge

Buzan B, Waever O, De Wilde J (1998) Security: a new framework for analysis. Lynne Rienner Publishers

Office Cabinet (2013) National risk register for civil emergencies. The Stationary Office, UK

Carlberg A (2008) Concepts on ethics. http://ec.europa.eu/research/participants/data/ref/fp7/89878/ethics-concepts_en.pdf. Accessed 5 May 2015

Chmutina K et al (2015) D7.1—report on North-West Europe regional workshop. Available at: http://evocs-project.eu/deliverables

Clarke M (1998) British security policy. In: Eliassen KA (ed) Foreign and security policy in the European union. Sage Publications, UK

Commission on Global Governance (2005) Our global neighborhood. Oxford University Press, New York

Commission on Human Security (2003) Human security now. New York. http://reliefweb.int/sites/reliefweb.int/files/resources/91BAEEDBA50C6907C1256D19006A9353-chs-security-may03.pdf. Accessed 7 May 2015

Council of Europe (1997) Oviedo convention. http://conventions.coe.int/Treaty/en/Treaties/Html/164.htm. Accessed 6 May 2015

De Nederlandse Grondwet (2015) http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrndb9f5vzi

DECC (2014) Digest of United Kingdom energy statistics

DHS Risk Lexicon (2010) http://www.dhs.gov/dhs-risk-lexicon

ETTIS consortium (2012) D1.1 conceptual foundations of security (ETTIS—European Security Trends and Threats in Society), European Security Trends and Threats in Society, see http://ettis-project.eu/wp-content/uploads/2012/03/D1_12.pdf

ETTIS consortium (2013) D1.2 a working definition of societal security (ETTIS—European security trends and threats in society), European security trends and threats in society, see http://ettis-project.eu/wp-content/uploads/2012/03/D1_2.pdf

European Commission (2011a) Internal security, special Eurobarometer 371. http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf. Accessed 6 May 2015

European Commission (2011b) Commission staff working paper—risk assessment and mapping guidelines for disaster management. http://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vilsc7ikt7zq

European Commission (2011c) The food security thematic programme. https://ec.europa.eu/europeaid/sectors/food-and-agriculture/food-and-nutrition-security/food-security-thematic-programme-fstp_en. Accessed 27 May 2015

European Commissions (2013) The EU strategy on adaptation to climate change. http://ec.europa.eu/clima/publications/docs/eu_strategy_en.pdf. Accessed 27 May 2015

European Commission (2014) European energy security strategy. http://ec.europa.eu/energy/en/topics/energy-strategy/energy-security-strategy. Accessed 27 May 2015

European Commission (2015) Communication from the council to the European Parliament, the council, the European economic and social committee and the committee of the regions, The European agenda on security, Strasbourg COM(2015) 185 final, 28 Apr 2015, http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf . Accessed 21 May 2015

European Group on Ethics in Science and New Technologies (2014) Ethics of security and surveillance technologies. http://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologies-pbNJAJ14028/. Accessed 6 May 2015

European Union (2012) Charter of fundamental rights of the European Union, 26 October 2012, 2012/C 326/02. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN. Accessed 6 May 2015

Freeman M (2011) Human rights: an interdisciplinary approach. Polity Press, Cambridge

Government of Serbia (2009) Strategija Nacionalne Bezbednosti Republike Srbije. http://www.gs.gov.rs/doc/strategije/Startegija%20nacionalne%20bezbednosti.docx. Accessed 12 May 2015

HM Government (2010) A strong Britain in an age of uncertainty: the national security strategy. The Stationary Office, UK

Hursthouse R (2012) Virtue ethics. In: Stanford encyclopedia of philosophy. http://plato.stanford.edu/entries/ethics-virtue/. Accessed 5 May 2015

Jonas H (1984) The imperative of responsibility. University of Chicago Press, Chicago

Jovanovic M, Petkov V, Radziejowska M, Todorova A (2014) D8.1—report on the regional workshops. Available at: http://evocs-project.eu/deliverables

Kant I (1785) Fundamental principles of the metaphysic of morals. http://www.gutenberg.org/cache/epub/5682/pg5682.html. Accessed 5 May 2015

Kymlicka W (2007) Multicultural odysseys: navigating the new international politics of diversity. Oxford University Press, Oxford

Lipman M (2003) Thinking in education, 2nd edn. Cambridge University Press, Cambridge

Loretoni A (2014) Ampliare lo sguardo. Genere e teoria politica. Donzelli, Roma

Ministerie van Veiligheid en Justitie (2007) Strategie Nationale Veiligheid. Rijksoverheid, Nederland

Ministerie van Buitenlandse Zaken (2013) A secure Netherlands in a secure world. Rijksoverheid, Nederland

Ministerie van Buitenlandse Zaken (2014) Beleidsbrief Internationale Veiligheid "Turbulente Tijden in een Instabiele Omgeving". Rijksoverheid, Nederland

MI5 (2014) Protecting national security. Available at: https://www.mi5.gov.uk/home/about-us/what-we-do/protecting-national-security.html. Accessed 20 Apr 15

NCTV (2014) Risico en crisis barometer, https://www.nctv.nl/actueel/nieuws/risico-en-crisisbarometer-oktober-2014.aspx, Rijksoverheid Nederland

Nussbaum M (2001) Women and human development. The capabilities approach. Cambridge University Press, Cambridge

Nussbaum M (2010) Not for profit. Why democracy needs the humanities. Princeton University Press, Princeton

Nussbaum M (2011) Creating capabilities: The human development approach. Harvard University Press, Harvard

Nussbaum M, Sen A (eds) (1993) The quality of life. Oxford University Press, Oxford

Oosterveld W et al (2015) The value of cooperation: innovation in Dutch security in perspective, the hague security delta, The Hague, https://www.thehaguesecuritydelta.com/images/The_Value_of_Cooperation.pdf

Pulcini E (2013) Care of the world: fear, responsibility, and justice in the global age. Springer, Dordrecht

Rawls J (1971) A theory of justice. Belknap Press of Harvard University Press, Cambridge

Reis Monteiro A (2014) Ethics of human rights. Springer, Dordrecht

Ricoeur P (1992) Oneself as another. Chicago University Press, Chicago

Schön D (1983) The reflective practitioner. How professionals think in action. Basic Books, New York

Sen A (1979) Equality of what? Tanner lectures on human values, Stanford University

Sen A (1985) Commodities and capabilities. North-Holland, Amsterdam

Sen A (1999) Development as freedom. Oxford University Press, Oxford

Sweijs T et al (2015) ASSESSING evolving concepts of security: coding handbook, deliverable 3.1. see http://evocs-project.eu/deliverables

Sweijs T (2009) Dutch military intervention making revisited, The Hague Centre for strategic studies, http://www.hcss.nl/reports/dutch-military-intervention-decision-making-revisited-getting-a-constitutional-grip-on-21st-century-wars/28/

Tadjbakhsh S, Chenoy A (2007) Human security: concept and implications. Routledge, London

United Nations (1992) An agenda for peace, preventive diplomacy, peace-making, peace-keeping: report of the secretary general, 17 June 1992 (A/47/277)

United Nations Development Program (1994) Human development report. Oxford University Press, New York

United Nations General Assembly (1948) Universal declaration of human rights, 10 December 1948, 217 A (III)

United Nations General Assembly (1993) Vienna declaration and programme of action, 25 June 1993, A/CONF.157/23

United Nations Trust Fund for Human Security (2009) Human security in theory and practice: application of the human security concept and the United Nations trust fund for human security. UNOCHA, New York

Weinblum S (2010) Beyond the security vs. liberty paradigm: A new look on security politics. In: Peled Y, Lewin-Epstein N, Mundlak G, Cohen J (eds) Democratic citizenship and war. Routledge, London

Wolters G (2015) Globalizzazione del bene? Orthotes, Salerno

National Security in a Hyper-connected World

Global Interdependence and National Security

Christian O. Fjäder

Abstract The objective of this chapter is to explore the opportunities and threats this hyper-connectivity presents to national security, specifically from an economic security point of view. How can national critical societal functions and infrastructures be secured against transnational and extra-sovereign dependencies that extend beyond the mandate of sovereign states? Moreover, how can a nation secure its external “lifelines” without violating the sovereignty of states these reside in or pass through? In the theoretical level these questions relate to the sovereign state’s autonomy of action in economics and national security in a system that increasingly functions on transnational and extraterritorial logic.

Keywords National security · Critical infrastructure protection · Resilience · Economic security · Globalization

1 Introduction

The concept of national security for a modern nation-state is now widely accepted to include a number of “soft” aspects of human security, including the responsibility to ensure the well-being, economic prosperity and happiness of citizens. An important field in this context is economic security, which includes efforts towards securing a nation’s industrial and technological base critical for national economy, security and defence, access to critical materials and resources and the functioning of critical infrastructures and services that are required for critical societal functions. Given the constantly increasing dependence of a modern nation-state on global flows and networks for the resources and knowledge—such as goods, services, people and information—required for the provision of the positive political goods to its citizens, without a constant and stable access to these resources a nation-state

C.O. Fjäder (✉)
The Finnish Institute of International Affairs, Helsinki, Finland
e-mail: Christian.fjader@fiia.fi

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_3

will not be able to maintain a competitive national economy, nor increasingly, effective national security. The global flows and networks providing these resources, and the global commons—the seas, air, space and the cyber domain—that provide the required channels for them, however, reside outside the borders of the nation-state and thus, outside their realm of control. National security interests have never been entirely limited by sovereign territory, but the intensity and complexity of the network of connections a modern nation-state depends on is blurring the distinction between internal and external aspects of national security (i.e. national and international) to an extent never seen before.

The objective of this chapter is to explore the opportunities and threats this hyper-connectivity presents to national security, specifically from an economic security point of view. How can national critical societal functions and infrastructures be secured against transnational and extra-sovereign dependencies that extend beyond the mandate of sovereign states? Moreover, how can a nation secure its external "lifelines" without violating the sovereignty of states these reside in or pass through? In the theoretical level these questions relate to the sovereign state's autonomy of action in economics and national security in a system that increasingly functions on transnational and extraterritorial logic.

In terms of national security, they relate to the manner nation-state deals with internal and external aspects of security and thus, questions on how should states bridge the nexus between economic security and national security in the strategic level. More specifically the chapter will address the opportunities and restraints for a nation state to establish a holistic security strategy to secure national critical societal functions and infrastructures against strategic risks relating to extra-sovereign dependencies. In this context cyber security is of increasing strategic importance, not least because it is arguably the field in which internal and external aspects of national security are most interrelated.

Finally, it will argue that in order to secure its access to global networks and flows, the governments will need to further link disparate policy realms, e.g. economic, security, defence and foreign policy, closer together into a holistic global strategy to secure its place in the global system it depends on.

2 National Security in the Age of Hyper-connectivity

The age of hyper-connectivity, whilst the talk of the town at Davos, also sounds ominously as hype talk to a regular person. However, if you consider the potential transformations it suggests in relation to the role of the nation-state, economy, business and the society at large, it becomes evident that "hyper-connectivity" will potentially have dramatic impact on them and consequently, on national security. Whilst there is no universal definition for "hyper-connectivity", it tends to refer to a not-too-distant future in which people, information, all kinds of "things", objects and infrastructure are ubiquitously connected to the Internet and via networks to each other. The first and most obvious characteristic of this "hyper-connectivity" is the enormous numbers of individual users across virtually every corner of the world it involves. Currently (as of January 2015) over 3 billion people across the world enjoy at least some access to the Internet, a number that is expected to rise to 4 billion by 2020 (Neowin 2013). However, the growth of the mobile Internet has brought connectivity accessible to populations across the world, the penetration levels are nonetheless much higher in the developed countries. For instance in Myanmar just 1.2 % of population has access, in comparison to developed countries where penetration rates vary between 70 and 90 % (EIU 2014). Whilst the Internet is indeed global in nature, penetration rates nonetheless still vary considerably between regions. For instance, penetration rate in North America is 88 and 81 % in Western Europe, whilst in Africa it is 26, 19 % in South Asia and 36 % in the Middle East. Considering the variance in regional penetration levels, and that the global penetration level is still only 42 % (We are Social 2015), it is rather clear that future growth is going to originate from outside of North America and Europe, the two regions that have thus far dominated the global internet infrastructure and governance in the cyber domain. What the implications of this will be for the security and governance of the global cyber domain remains to be seen.

However, the more drastic development is the "Internet of Things" (IoT), or as it is sometimes called, the "Internet of everything", "Industrial Internet" or "Internet everywhere", could result in more than 50 billion "things" to become connected to the internet by 2020 (WEF 2012). Whilst the definition of "Internet of Things" is elusive in general, the use of the term refers to the use of sensors and data communications technology built into physical objects in order to track, coordinate or control the functioning of those objects based on data over the network or the Internet (MGI 2013: 52). Whilst the physical objects range anything from cars to coffee and washing machines, it is expected that the industrial Internet will include all kinds of manufacturing processes, as well as services, logistics and infrastructure maintenance ranging from anything from facilities management to management of electricity transmission and water distribution networks, as well as essential services such as healthcare, waste management and transportation. Any object previously thought as "dumb", will be able to monitor, communicate and respond with their changing environment. At least in theory, the possibilities are endless. Goldman Sachs has divided the potential application of IoT into five areas:

1. Connected wearable devices
2. Connected homes
3. Connected cities
4. Connected cars
5. The Industrial Internet (Value Walk 2014)

The extent of the IoT is not, however, limited to inanimate "things", but significantly it holds to promise to bridge the divide between machines and living "things" (humans and animals). Moreover, it could facilitate automatic and autonomous data-based processes without requiring human intervention. The definition by Telecom Circle reflects this notion:

> The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers and the ability to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction (Telecom Circle 2014).

One illustrative example of such automated and autonomous processes is High Frequency Trading (HFT). HFT, or "algorithm trading", relies on powerful computer platforms running complex algorithms to analyse multiple markets and a very large number of orders at very high speeds (in milliseconds), (Ivestopedia 2014) thus profiting from optimal prices. This is clearly a level of performance beyond what human traders could accomplish. On the other hand, as the "flash crash" of 2010 demonstrated, if great profits to be made in milliseconds, the same applies to losses. The "flash crash" produced the biggest stock market plunge in decades when Dow Jones Industrial Average suffered a 1000 point loss (equalling to 9 % of market value) in just 5 min. Following an investigation it was eventually discovered that a single trader from the UK- Navinder Singh Sarao—was allegedly a major factor behind the incident. The investigation established that Sarao used an automated trading program to manipulate contracts known as e-minis, which contributed to the crash. Sarao has since been charged with multiple accounts of wire fraud, commodities manipulation and spoofing. The disturbing fact is that the "flash crash" could well happen again, due to variety of causes, e.g. computer of algorithm malfunctions, hacking or perhaps through social media manipulation of the markets (Forbes 2013). What is rather certain in any case is that the volumes involved in HFT are increasing. BlackRock, the world's largest fund management firm, with total assets under management valuing at US$4.77 trillion (Blackrock 2015), is developing a new firm-wide trading system to leverage on the potential of HFT. BlackRock, however, insists that it is against predatory use of HFT and will act responsibly in the use of computer algorithm assisted trading (Blackrock 2014).

The economic impact of the Internet and especially IoT, is expected to be enormous and overarching. First of all, according to Deloitte, if countries in Africa, Latin America, South and East Asia would reach the same level of Internet connectivity that exists in the developed countries, it could boost the long-term productivity of the world economy by 25 %, the GDP growth rate by 72 % and create an additional 140 million new jobs (EIU 2014: 5). The full emergence of IoT's potential, on the other hand, is expected to add US$14.2 trillion to the global economy by 2030 (Accenture 2015). Consequently, IoT is likely to alter the logic of business and have a tremendous impact on the global economy. It will also most likely offer both new opportunities and risks with direct implication on security.

The impact of hyper-connectivity, however, stretches beyond economics and business, potentially remoulding the social fabric of societies and quite possibly politics. Above all, however, it will alter the allocation of responsibility for risk, in particular systemic risk. A joint report by the World Economic Forum and Deloitte—*Risk and Responsibility in a Hyperconnected World*—for instance states that:

> Digital technology touches virtually every aspect of daily life today. Social interaction, healthcare activity, political engagement or economic decision-making – digital connectivity

> permeates it all, and the dependence on this connectivity is growing swiftly. Greater reliance on a networked resource naturally makes us more interdependent on one another. As the new, shared digital space evolves, the collective imperative is to develop a common set of expectations to address systemic risks, and to define not only the roles but also the responsibilities of all participants in the cyber ecosystem. (WEF 2012: 5)

The impacts of hyper-connectivity to nation-states in general can be potentially transformative in nature. In the minimum it most certainly accelerates globalization and thus, further removing the restricting effect of borders and facilitating more transnational processes taking place in extra-sovereign domains. The first and most obvious of course economic activity, which with the emergence of the global digital marketplace, appears to be rapidly beyond the control of the state and hence, ultimately lead to a collapse of the state's economic pillars of power. As companies become increasingly global citizens and economic boundaries no longer correspond with the political borders, the role of the state is bound to decline. Moreover, not only governments are losing their agency in international trade, but as individuals can also trade directly globally without the companies acting as middlemen, the corporation as an intermediary of economic activity will also lose its.

2.1 The Interdependent World: The Nation-State's in a "Borderless World"

The globally connected and interdependent world was first presented in International Relations theory by Robert Keohane and Joseph Nye Jr. in their seminal book Power and Interdependence in 1977, and in particular in its updated version Power and Interdependence in the Information Age in 1998, in which they depict an international system bound together by a web of complex interdependencies which on the whole benefits all parties involved. This neoliberal world of "complex interdependencies" was expected to result in a world where security and force matter less. Neoliberalism, like its competing paradigm—neorealism—acknowledges the anarchic nature of the international system, but argues that it can be alleviated by cooperation. In general neoliberalism has a tendency to emphasize the positive outcomes of interdependence and interconnectedness, rather than the possible risks and vulnerabilities. Moreover, whilst it is a rationalist and state-based approach, neoliberalism places great value on non-state actors. This also extends to the role of non-state actors in security, both as sources of threats and as providers of security. Neorealism, on the other hand, has a tendency to argue that the nation-state has remained the principal agent in security, in particular, in terms of accountability, despite the advancement of globalization and the proliferation of transnational threats and actors (Ripsman and Paul 2010: 10). The realist paradigm emphasises Hobbesian survival in an anarchic international system. This approach, however, reflects poorly the reality of transnational actors in these critical functions and security, increasingly operating in extra-sovereign domains. On the other hand, the parties involved also become more dependent on continuous access to these flows (Milner 2009: 15). Consequently, specifically from the point of view of a nation-state, the increasing web of interdependencies can also be seen as a source of broadening and deepening dependency on extra-sovereign resources, networks and connections. Such connectivity also potentially brings new risks, as the project of making Singapore a global hub so vividly demonstrates (Heng 2013) and in the system-level what Dillon call as "problems of circulation" (Dillon 2005: 2). Dirk Helbing, on the other hand, argues that systemic failures and extreme events are consequences of highly connected systems and networked risks and that a hyper-connected world is increasingly likely to see the emergence of hyper-risks as a result of complexity of these "complex interdependencies" (Helbing 2013).

For the nation-states the reality of global interdependence is also emerging as a national security issue. In this context "dependence" is perceived as the antonym of independence, which in the state-centric approaches translates into state sovereignty, and thus challenges sovereign control over resources critical for national security. In the context of national security dependency is typically perceived as representing a vulnerability, which must be mitigated somehow. Interestingly, however, it would seem that in the context of economic security, the neoliberal and neorealist ontologies coexist in apparent harmony.

However, it could be argued that neither paradigm has placed adequate attention and value to the emerging interplay between the nation-state and transnational actors, the nation-state's responsibility to secure critical societal functions in a reality where they increasingly depend on or operate in extra-sovereign domains. Moreover, since both are state centric and rationalist approaches, they also have a tendency to place inadequate attention to non-state actors not only as challengers, but also providers of security. On the other hand, state space is becoming increasingly multi-scalar in nature, as well as increasingly networked and depending on context, prompting the need to think sovereignty as a relational process rather than in a state territorial frame (Moisio and Paasi 2013: 257). This in turn would suggest that national security cannot for much longer be neatly separated between internal and external and between hard and soft power. Dealing with extra-sovereign dependencies that can challenge national security simply requires a new ontology and fresh new approaches. Finally, in the system-level, the distinction between "interdependence" and "dependence" warrants further thought. Whilst this has been approached from the point of view of relational power (Keohane and Nye 1997), the emerging national security dependencies on extra-sovereign domains prompts us to reconsider what are dynamics between that of "interdependence", which could be even seen as a source of resilience, and the genuine raw "dependence" that suggest loss of sovereign autonomy and emerging systemic risks that could suggest the rise of geo-economics as a new paradigm for relational power and thus, challenge the neo-liberal world order.

2.2 *From Hobbesian Survival to National Security in an Interconnected World*

The transition of national security to the globally interconnected world, however, is neither easy nor natural. National security has traditionally focused on ensuring the sovereignty of the nation-state by maintaining security bureaucracies that are tasked to protect the state and its citizens from external and internal threats within a geographically defined territory (Ripmans and Paul 2010: 11). The traditional concept of national security derives its origins from a line of modernist political and sociological thought from Thomas Hobbes to Max Weber, insisting that the state needs to have the absolute monopoly upon the legitimate use of physical force and that security is the core responsibility of a nation-state.

The emergence of the welfare state after WWII introduced a new type of a protective state that aimed to guarantee the welfare of its citizens by offering social services, health care, education and social benefits in the form of the provision of social security and unemployment benefits. As a result of this evolution, the modern nation-state's core responsibilities are now seen to focus on the provision of positive political goods, such as security, health care, education, law and order, economic opportunity and critical infrastructure, i.e. the protection of the overall well-being of its citizens. As such the state maintains a central role in the economic, political, social and cultural life of its citizens that is both pervasive and persistent. The inclusion of new security threats, however, principally non-military threats, mostly posed by non-state actors, such as international terrorism, organised crime, pandemics, natural disasters, drug trafficking and people trafficking, into the national security agendas, presented the state with both new challenges and, arguably, new opportunities. If globalisation has been seen to transform the role of the nation-state, in a similar manner it has been argued as having transformed the concept of national security. Consequently, it has been suggested that the provisioning of security has become increasingly difficult for the nation-state, as its span of control does not efficiently correspond with the transnational threats at the heart of this emerging uncertainty.

Barry Buzan, however, argues that despite the declining role of the state in the management of the economy, the state still remains the principal security provider because it is the only societal organisation that has both the capacity to act and the authority to define what represents a security threat. Since there is no global government or society that could replace the nation-state, the nation-state is simply the best available institution to take its place (Buzan 2007). Moreover, Keith Krause argues that in fact the role of the state has expanded, due to the securitisation of non-traditional threats. Consequently, the responsibilities of the state now include protecting citizens from the threat of violence and creating not only the conditions for economic and social well-being, but also for the preservation of their core values and identity. Furthermore, Krause argues that states seek to distinguish the 'national security' agenda from the more day-to-day political 'problems' by emphasising the urgent, existential or pervasive nature of security threats (Krause 2007). Hence, at least partially due to the securitisation of non-traditional threats, the nation-state has managed not only to maintain its mandate to regulate security, but to decide what constitutes a security issue and through the mandate to define the national interest, to dictate the agenda for national security.

2.3 Economic Security in a Hyper-connected World

With the expansion of the concept of national security and securitization of the functions of the economy, the calls for "economic security" appear to be proliferating again. Albeit the "original" use of the term—security national security and defense through economic means—still persists, the term is also increasingly used in the context of response to economic risks, unexpected shocks and economic volatility towards security the sovereign autonomy in globally interdependent world. Such concerns have prompted calls for a new definition for economic security in an era of globalization (e.g. Kahler 2004). Whilst such a definition is still a work in progress, in the context of national security "economic security" has emerged to cover the external and internal, soft and hard aspects of security, and includes such disparate measures and policies as security of supply, market-access security, access to finance, trade route access and systemic level and socio-economic security. The definition presented in a RAND report on economic aspects of national security captures this variety, albeit with a specific "rich super-power" flavor. It is, nonetheless, an illustrative example of an attempt to integrate internal and external, soft and hard and economic and security goals and means (security for economic resources vs. economic resources to security) into one holistic bundle:

> Economic security is the ability to protect or advance U.S. economic interests in the face of events, developments, or actions that may threaten or block these interests. These challenges or obstacles may be foreign or domestic in origin, intentional or accidental, and the consequences of human or natural forces. Further, economic security depends on the United States' ability to shape the international environment to its liking – for example, by playing a major role in establishing the rules that govern international economic relations by using economic means to influence the policies (economic or otherwise) of other countries. Economic security also requires possessing the material resources to fend off non-economic challenges (Neu and Wolf 1994).

The statement is, however, also an illustration of the difficulties a modern nation-state has to tackle in defining its national security objectives in an actionable manner in a constantly broadening and changing security agenda. Whilst economic security has traditionally focused on ensuring that national security and defense have the required resources, principally by designated domestic strategic industries, with the expansion of the concept of national security, "economic security" has evolved to cover also the economic well-being of the population and opportunities for businesses and citizens to provide for their own essential needs. Consequently, the use of the concept has not only expanded, but it has also (intentionally or unintentionally) shifted from hard to soft concepts of power and security, as well as from relatively specific scope to a systemic-level scope that blends also macro- and microeconomic aspects. The macroeconomic aspect focuses on securing system stability in order to ensure economic growth and prosperity, whilst the microeconomic focuses on resources and capabilities that act as enablers, e.g. science and technology, education, business methods and natural resource use (Nanto 2011). In terms of the external use of economic security, the focus has shifted more towards the use of soft power, aiming at securing the global economic stability, functioning of the international financial system and the continuity of and access to the international trade and investment flows. Consequently, economic security is increasingly characterized by increasingly diversified goals and measures and is becoming increasingly challenging even in the safety of the sovereign container of a nation-state.

The policy response to this emerging dilemma has been one of a mixed bag. On the one hand, under "business as usual" conditions the assumption tends to be that "markets will handle it". On the other hand, when threats emerge or disruptions materialize, the issue quickly becomes a question of national security. Much of this is related with the realization that national economies are not isolated, the concept of power is evolving, economic power plays a more central role in it and that economies and critical societal functions are becoming more intertwined.

The emerging challenges "hyper-connectivity" possibly presents to economic and national security are diverse. The first is the sheer volume of connections involving more people, devices and things being connected to more things and each other. The second is ubiquity; everything is going to be connected and connections are everywhere. The criticality of this reality largely depends on the depth versus breath of hyper-connectivity. Whilst the basic assumption that everything is going to be connected may well hold, what the depth of dependence on these connections will be in the physical world is going to be critical for what kind of vulnerabilities and risks will emerge. Thirdly, the speed of transactions may pose its own challenges. In the "Internet of everything" digital transactions can happen in a span of milliseconds. A good example of this is the High Frequency Trading (HFT) highlighted earlier. Finally, the sum total of hyper-connectivity is complexity. The multitude of connections, the dynamic and contextual relations between the connected systems and processes and the complex value chain of resources, owners and operators behind them makes it increasingly hard to determine what depends on what, who is responsible for what and in particular—who takes responsibility for risk and security.

The impacts of this emerging reality on national security are that visibility to threats is going to decrease as processes increasingly are executed in extra-sovereign domains or are dependent on information residing in them. Moreover, within a complex web of almost instantaneous transactions the actors are not easily identifiable, not to mention their intentions. Consequently, an increasing amount of activity that could potentially threaten national security, either purposefully or coincidentally, is going to be beyond the span of control of nation-states and their security bureaucracies. The threats in the hyper-connected world are thus increasingly multifaceted, whilst national security operates in silos (e.g. hard and soft security), and more instantaneous, whilst government decision-making structures and cultures are not equipped towards real-time.

3 Critical Infrastructure Protection in a Hyper-connected World

An increasingly important field of national security is Critical Infrastructure Protection (CIP), the policy field dedicated to the protection of national critical infrastructure, which delivers, enables and supports the provision of critical services to the citizens, communities and the economy. CIP relies on definitions of ‘critical’ and, thus, that of ‘critical infrastructure’, for its scope and mission.

Whilst these definitions vary from country to country, in most cases ‘critical’ refers to infrastructure that provides life sustaining and essential services required for the economic and social well-being of citizens, national and public security and key government functions (OECD 2008). The sectors typically considered as critical infrastructure are: energy, water services, communications, transport, food supply chains, health, banking and finance, national security and defence-related assets.

The definitions of ‘infrastructure’ still tend to focus on physical infrastructures, but some countries now also include intangible assets, such as supply chains that enable the functioning of physical infrastructure and/or deliver critical services (OECD 2008: 6). For instance, the Australian government’s Critical Infrastructure Resilience Strategy (2010) defines critical infrastructure as:

> … those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia’s ability to conduct national defence and ensure national security. (Australian Government 2010)

In a similar spirit, the UK Government defines the Critical National Infrastructure (CNI) as:

> Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life (UK Cabinet Office 2010).

In a world of hyper-connectivity, however, such definitions of critical national infrastructures have serious limitations for national security, as the following sections will demonstrate.

3.1 Critical Infrastructure Protection: Securing Transnational Dependencies

The concept of national critical infrastructures is not new and has been a strategic security issue at least from World War II onwards. For instance, the US Strategic Bombing Survey (1944–46) determined what enemy critical infrastructures rewarded bombing in order to reach strategic war objectives. During the Cold War both sides surveyed each other's critical infrastructure for strategic targeting purposes. Consequently, national CIP policies were mostly focused on protecting government sites and key facilities against attack, whilst anything else was the concern of local-or regional-level authorities (Chatham House 2013: 8). The strategic underlining assumption and focus was thus very much in line with traditional territorial defence of a sovereign state. As noted before, the scope of what is being protected and against what has considerably expanded since. Moreover, a significant development within the context of this research, the international dependencies have more recently multiplied and become global to the extent that it is becoming increasingly difficult to define the defensive perimeters within the context of territorial sovereignty (Chatham House 2013: iv). The emergence of global supply and value chains, privatisation of industries and services traditionally considered as strategic national assets. Moreover, critical infrastructure is not only increasingly privately owned and operated, but in many cases also owned by foreign corporation or even governments. Even if they are not foreign owned and operated, or are even owned by the national government, practically all depend on the global value chains for their daily functioning. The nature and extent of the dependencies obviously vary greatly, but it is rather safe to assume that at least some resource, information or process dependencies extent beyond national borders.

The response to this emerging reality has, however, been rather ambiguous. Most national security or critical infrastructure protection related strategies refer to the international or global operating environment and hence, increasingly acknowledge the growing challenge of international dependencies, but in general do not provide a concrete path for addressing these. Instead, most national strategies and programmes focus on interdependencies between various CI sectors, vulnerabilities, threats and risks concerning them and public-private cooperation in critical infrastructure protection. This is a result of emphasising the criticality of assets and structures, based on the notion that e.g. water systems, electricity grids, telecommunication networks and even cyber assets rely on physical structures (e.g. ports, airports, plants, sites, cables, masts, base stations, switches, etc.) that are generally seen as local. Whilst the physical structures clearly are (mostly) local in a sense that they reside in a given territory, the resources enabling and supporting them are not necessary local at all, but instead can originate in the other side of the world. Moreover, these dependencies are not only related to resources and materials, but increasingly include the information, (remote) technical support and maintenance processes and services, that are globally spread in order to maximise cost efficiencies provided by the global value chain. In many cases the physical connection between systems extend beyond borders, e.g. electricity transmission networks or the international submarine cables that carry majority of global internet and telecommunications traffic, without which the global internet and the local systems connected to it could not operate.

The growing concern over the international aspects of CIP is nonetheless evident in an increasing number of national security strategies (e.g. Australia, Canada, Netherlands and the United States), but also in the European Union, as embodied in the European Union Council Directive on European Critical Infrastructures (2008) and the European Programme for Critical Infrastructure Protection (EPCIP), which sets an EU-wide framework for "activities aimed at improving the protection of critical infrastructure in Europe—across all EU States and in all relevant sectors of economic activity" (EC 2015). The directive is somewhat of an achievement in the field, in particular concerning that it passed despite the limitations of the subsidiarity principle. The principle of subsidiarity is intended to regulate the executive power of the EU by determining whether an issue meets the criteria of "joint competence", or if it should be left for the sovereign decision-making of the member states. In regards to the CIP directive, the European Council determined that in this case the issue met the criteria "…because the transnational risks of interference with European critical infrastructure can cause disruption to more than one member state" (Chatham House 2013: 8). The European Union defines CI as an asset, "system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" (EU 2008).

The EU directive acknowledges an increase in transnational, and indeed, global dependencies in critical infrastructures and proposed five types of interdependencies: (1) physical, (2) information, (3) geospatial, (4) policy and process and (5) societal. Special emphasis was put on the energy and transport sectors. Criteria for these European Critical Infrastructures (ECI) was that a disruption of such infrastructure in one member state could impact two others in a critical manner.

Similar notions are present in some of the national strategies published. Britain's national security strategy—A Strong Britain in the Age of Uncertainty'—for instance states that Britain is more vulnerable to global threats 'because we are one of the most open societies, in a world that is more networked than ever before'. It also refers to a multitude of new threats, including those posed by non-state actors, e.g. terrorism, security of national energy, food and water supply and climate change as the sources of threat to Britain's national security (HM Government 2010). Following a similar logic, Canada's national security policy—'Securing an Open Society: Canada's National Security Policy—states:

> There can be no greater role, no more important obligation for a government, than the protection and safety of its citizens. But as all Canadians know, we live in an increasingly interconnected, complex and often dangerous world (Government of Canada 2015).

Canada's most recent economic action plan, on the other hand, addresses the critical infrastructure shared with the United States and proposes programs to jointly enhance resilience of shared critical infrastructures. The plan also includes a pilot project that would produce a joint regional resilience assessment and risk analysis for the Maine—New Brunswick region (Government of Canada 2015).

The Netherlands has also adopted an overarching international security strategy in order to respond to large-scale and rapid changes in the global system, whether they are economic, political or security related in nature. The strategy underlines uncertainty and the difficulty to distinguish between internal and external security in this new reality (Government of the Netherlands 2013).

In the United States the Homeland Security Act of 2002 defines "key resources" as the "publicly or privately controlled resources essential to the minimal operations of the economy and government". Apparently transnational dependencies are identified and assessed by a joint State Department—DHS project called Critical Foreign Dependencies Initiative (CFDI), according to documents leaked to Wikileaks. The project reportedly aims to identify resources around the world that were to be considered critical for the public health, economic security, and/or national and homeland security of the United States, and includes diverse assets, such as submarine telecommunications and internet cables, pharmaceutical manufacturing and global supply chain nodes—e.g. major ports and critical sea-lanes (BBC News 2010). In other words, the program focuses on the transnational and extra-sovereign structural dependencies of national key resources, as well as the critical connections to them.

How such global critical dependencies and interdependencies would be addressed in concrete terms is still mostly an open question, as multilateral CIP cooperation is still very limited. Perhaps the most significant multilevel forum specifically dedicated to such issues is currently the EU-US-Canada Expert Meeting on Critical Infrastructure Protection, which brings together experts from DHS, Department of Public Safety Canada and their counterparts in the EU member state to exchange information on strategic policy-making issues on critical infrastructure protection matters. The 2015 meeting in Latvia also addressed the foreign policy dimension of CIP, albeit mostly focusing on transnational flows between neighbouring states (EU 2015).

3.2 The Global Supply Chain and National Security

> International trade has been and continues to be a powerful engine of United States and global economic growth. In recent years, communications technology advances and trade barrier and production cost reductions have contributed to global capital market expansion and new economic opportunity. The global supply chain system that supports this trade is essential to the United States' economy and security and is a critical global asset. The Whitehouse—National Strategy for Global Supply Chain Security (2012)

There is little doubt that the emergence of global supply chains has transformed the world economy by significantly lowering the cost of transportation, breaking the tyranny of proximity between production and the end-customers and thus, enabling economies of scale for larger volumes of production and specialisation though offshoring and vertical integration, leading to end-to-end global integration of production and business processes across the world into Global Value Chains (GVCs) that have little respect to sovereign borders. As such it has become the engine room of the contemporary global economy, without which many of the products and services that we have grown used to would not be so easily and cheaply available across the globe.

The global supply chain is genuinely enormous—the global flows of goods, services and finances reached a total value of US$26 trillion in 2012, accounting for 36 % of global GDP. Each year the global flows add approximately US$450 billion to the global economy. The McKinsey Global Institute estimates that if the process of digitalisation progresses as predicted it will further break down the barriers for participation and the value of global flows could almost triple by 2025 (MGI 2013: 109). The total value of the entire global supply chain is, however, in fact hard to establish, as its reach extends well beyond trade in goods and services and financial flows, including variety of services to economies and businesses that would not otherwise exist, e.g. international investment in production, infrastructure services, logistics, telecommunications, trade related finances and increasingly, the Internet.

The participation rates between countries obviously still vary considerably, in particular between advanced and emerging economies. The McKinsey Global Institute Connectedness Index, measuring the participation of countries in global flows in relative terms, places Germany on top, followed by Hong Kong and Singapore. In terms of differences in participation rates between countries with different levels of economic development, it notes that even though the participation rates by emerging economies are growing, they still significantly lag behind developed economies, which have average rank of 21 against 77 in the emerging economies (MGI 2013: 62). The DHL Global Connectedness Index 2014 examines the connectedness of 140 countries based on the depth of their connectedness to global flows, their geographic distribution (breath) and their directionality (outward vs. inward flows). The report concludes that the level of global connectedness is in fact lower than many would think. Moreover, the most connected countries in the context of the depth of their connectedness tend to be primarily the wealthy and relatively small countries, e.g. Hong Kong, Luxembourg and Singapore. In terms of breadth of connectedness, the top ranking countries are also wealthy but somewhat larger economies, such as the Netherlands, which tops the overall ranking (followed by Ireland, Singapore, Belgium, Luxembourg, Switzerland, the United Kingdom, Denmark, Germany and Sweden) (DHL 2014: 8). It is worth noting that 9 out of 10 top countries are from Europe, albeit the report concludes that the connectedness of the advanced economies appears to be in decline, whilst that of the emerging economies is on the rise. Nonetheless, currently North America is the second most globally connected region after Europe, whilst Sub-Saharan Africa, South and Central Asia and South and Central America and the Caribbean are the least connected (DHL 2014: 9).

The flip-side with global connectedness is that countries with higher rates of connectivity probably need to worry more about significant disruptions as well. Some of the most referred to low probability—high impact events that have thus far caused significant disruptions in the global supply chains are the 9/11, Hurricane Katrina (2005), the Eyjafjallajökull volcanic eruption (2010), Tohoku earthquake and tsunami (2011), Thailand flooding (2012) and Hurricane Sandy (2012). None of these were predicted. Moreover, there is no reason to assume that events that have a similar level of magnitude would not take place also in the future. In addition to natural disasters, geopolitical risks, demand shocks, pandemics, cyber security and systemic vulnerabilities (e.g. oil dependency and information fragmentation) top the list of concerns (WEF 2013: 7). Whilst a joint report by the World Economic Forum and Accenture concludes that the global supply chains in general work well on daily basis, it also notes that according to a survey conducted by Accenture more than 80 % of companies surveyed were concerned over supply chain resilience as a major risk to their business (WEF 2013: 7). Consequently the report highlights proposed measures to be taken in order to enhance security cooperation across supply chain actors; the need for common risk vocabulary, improved data and information sharing and building greater agility and flexibility into resilience strategies (WEF 2013: 8).

A number of international initiatives have been established to address transportation and security risks after 9/11, principally the C-TPAT (Customs—Trade Partnership Against Terrorism), the Container Security Initiative (CSI), both led by the United States, as well as the Authorized Economic Operators (AEO) programme by the European Union. However, there is currently little focus on systemic risks within the global supply chain.

Such concerns were apparently the primary motivation for the United States government to establish a National Strategy for Global Supply Chain Security in Whitehouse 2012. The strategy states that:

> Through the National Strategy for Global Supply Chain Security, we establish the United States Government's policy to strengthen the global supply chain in order to protect the welfare and interests of the American people and secure our Nation's economic prosperity. Our focus in this Strategy is the worldwide network of transportation, postal, and shipping pathways; assets and infrastructure by which goods are moved from the point of manufacture until they reach an end consumer; and supporting communications infrastructure and systems (Whitehouse 2012).
>
> The strategy has two underlining goals: (1) to promote the efficient and secure movement of goods and services—protect these against exploitation and reducing vulnerability against disruptions and (2) to foster a resilient supply chain, which has the capability to withstand threats and hazards, recover from them and ensure the continuity of critical trade flows (Whitehouse 2012).

Such strategies, however, focus on securing nodes and processes, and do not yet adequately address the possible gap between national security and the growing dependence on these largely non-governed extra-sovereign domains.

4 Cyber Security and National Security: Securing the Global Cyber Domain

> America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas. President Obama (Whitehouse 2013)

As has already been suggested, information and communication networks have become a fundamental part of a nation's infrastructure, needed for economic stability and growth. The focus on the "digital economy" as a source of future economic prosperity and growth in an increasing number of economic strategies emphasises the benefits of hyper-connectivity—the efficiencies, cost effectiveness and new innovative business models that create new opportunities. The benefits can indeed be significant. For instance the emergence of "Smart Grids" in utility services could significantly benefit both the operators and consumers, as data-driven demand management based on real-time information can allow consumers to cut down their utility costs and the operators to reduce their operating costs through optimising balancing between demand and supply and regulating peak demand. Such solutions could also reduce outage times, as they would greatly assist operators to monitor and diagnose network problems in real-time (MGI 2013). These types of technologies hold the promise of doing the same to systems that societal processes depend on, what SCADA (supervisory control and data acquisition) systems have done to industrial processes, i.e. making them more effective and cost efficient.

Reaping the benefits from hyper-connectivity, however, requires continuous connectivity to the global value chains. Consequently, disconnection would endanger not only economic stability and growth, but could also have direct security impacts. Hence, it should not be a surprise that connectivity is rapidly emerging as a national security issue. As critical infrastructures become even more connected, even more distributed and complex cyber risks may well become a source of "hyper-risk". Such apocalyptic scenarios of a "digital Pearl Harbor" or "Cybergeddon" have in fact been predicted already since the 1990s, and were expected to cripple the entire society, disrupting anything from traffic lights to ATMs and public transportation, driving populations into panic and create chaos and mayham. For instance in 1997 Deputy Secretary of Defense—John Hamre—warned at the congressional hearing about such a scenario by stating that:

> We're facing the possibility of an electronic Pearl Harbor….There is going to be an electronic attack on this country sometime in the future (CNN 1997).

Similar warnings were voiced since by a number of officials and experts. For instance the Secretary of Defense—Leon Panetta—warned in 2012 that 'a cyber-Pearl Harbor' could bring down critical infrastructure and the government and cause loss of life, paralyze the nation and 'create a profound new sense of vulnerablity' (NYT 2012).

A "Cybergeddon" never happened, however probably because whilst the services where increasingly connected to networks, in most cases they were still at least somewhat separated from the physical world and allowed for human intervention. In fact, "Cybergeddon" proved to be somewhat of a lame duck in the years that followed as attacks were mostly narrowly focused and did not result in widespread and persistent disruption (Zurich Atlantic Council 2014: 14). This is not to underestimate the nuisance, harm and loss of revenue to an ever increasing amount of innocent victims variety of hacking and Distributed Denial of Service (DDoS) attacks have caused, but (fortunately) not a single event that would have caused widespread and persistent to the critical functions of the society has materialised despite the almost daily apocalyptic predictions of cyber the Nostredamuses. As Peter Singer has noted "over 32,000 scholarly articles have discussed cyberterrorism […] and 0 people have been killed by it" (Chatham House 2013: 8).

Before dismissing the possibility of a "Cybergeddon" in the future, however, it should be noted that the Internet is no longer merely a communications medium, but also increasingly a common and shared infrastructure upon which an increasing number of processes in the physical world rely. For instance if electricity distribution is disrupted because of a cyber event and service is consequently lost for an extended period time, in the worst case during the coldest winter period, people could actually die. Not because of a direct—kinetic—impact event, but because hospital systems and other utilities stop functioning as a consequence. For example, the U.S. Cyber Consequences unit has estimated that if electrical power was disrupted in a wide-enough area in the United States for over a week, up to 70 % of GDP could be lost, but even more seriously as generators would run out fuel and food stocks and other emergency supplies would have run out, people's lifes could be at grave risk (Zurich Atlantic Council 2014: 11). This is in fact entirely possible. For instance, Charles Perrow, a Sociology professor behind the concept of 'normal accidents' theory, has noted that we have produced so complicated designs of systems that we have lost the ability to anticipate "all the possible interactions of inevitable failures" and on top of that we have taken that complexity and plugged it into the Internet (Zurich Atlantic Council 2014: 14). The combination of systemic complexity and systemic risk could thus, cause widespread and persistent disruptive events that we do not have capability to anticipate.

The emergence of "cyber security" as a national security issue has led to a proliferation of national cyber security strategies across the world. The United States has been generally been credited as the first country to develop a holistic cyber security strategy in 2003, but was soon followed by a number of European nations. In Europe Germany released in 2005 a “National Plan for Information Infrastructure Protection”, followed by Sweden in 2006. Estonia, one of the most digitalised countries in the world was the first European nation to develop a holistic cyber security strategy in 2008, following the cyber attacks against Estonia in 2007 (ENISA 2012). Other developed nations that have released such a strategy include Australia (2011), Canada (2010) and Japan (2010), but also developing nations have released national strategies, e.g. India (2013), Kenya (2014), Namibia (2014) and Nigeria (2015).

The European Union released its “Cybersecurity Strategy of the European Union—An Open, Safe and Secure Cyberspace” in 2013. The strategy was motivated by a realisation of the Internet’s rapidly increasing importance for economic success and security, combined with a perceived lack of global governance. The strategy conveyed this notion in a rather dramatic language:

> The borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for requirements for transparency, accountability and security is becoming more and more prominent. (EC 2013)

The strategy aims at enhancing information sharing and coordination on incidents between EU member states, regulatory measures to enhance “cyber resilience” and enforced the mandate of the European Network and Information Security Agency (ENISA). It also proposed the shift adaptation of a Network and Information Security (NIS) directive that would further enhance EU’s cyber resilience (EC 2013).

In general such strategies seek to provide a national governance framework for cyber security, national goals for cyber security and seek to define the policy and regulatory measures required for reaching the goals. They also seek to provide a framework for the definition of national critical information infrastructures, their interdependencies, vulnerabilities and risks, as well as preferred frameworks for cyber preparedness, response and recovery. The role of public engagement and awareness, exercising and testing, education and competence building and standards, as well as research and development are pointed out as critical. Practically all refer to international cooperation, but few provide any level of detail as to what it actually entails.

This unavoidably brings up the question of what we really mean by “cyber security’s”, and in reference to critical infrastructure, what new it brings to the table in comparison to Critical Information Infrastructure Protection (CIIP)?

The definitions for cyber security tend to focus on the confidentiality, integrity and availability of information residing in information systems or being transmitted via the cyberspace (NATO 2015). Such definitions, however, offer little new in comparison to the already well-established and widely spread information security standards that have focused on exactly the same measures. A Chatham House report suggests a framework that could be helpful in this regard; it argues that "cyberspace" can be divided into several categories that include physical, logical and societal layers (Chatham House 2013: 4). The societal layer nonetheless tends to remain ambiguous and hard to define in a similar level than the other two.

Nonetheless, some countries have started to link the reliability of the cyberspace to critical infrastructure/vital societal functions and the consequences of cyber events on these. For instance, the Finnish national cyber security strategy states that:

> Cyber security encompasses the measures on the functions vital to society and the critical infrastructure which aim to achieve the capability of predictive management and, if necessary, tolerance of cyber threats and their effects, which can cause significant harm or danger to Finland or its population.[1]

The expansion of national security into the cyber domain and the expansion of the concept of critical infrastructures is likely to lead into similar definitions in other countries in the future.

4.1 National Critical Information Infrastructure and the Global Internet

> "…a defensive perimeter or outsourced inside, whereby the contiguous nation-state becomes fragmented into a discontiguous networkstate, its points never in direct physical contact. It is thus not a constitutional entity in any recognized sense, but a coordinated infrastructural ensemble that spans whole continents at a time (Chatham House 2013: 22).

The first and foremost challenge with national cyber security is to determine what "national" information infrastructure actually is—is it limited to the physical components, software assets, connections and connectivity that reside within the sovereign boundaries of the nation-state, or does it include resources and information in the extra-sovereign cyberspace? The first aspect is usually covered in the context of CI sectors. The extra-sovereign aspect, however, remains a strategic challenge. The traditional approach has been to create a protective layer isolating the two from each other, by for instance restricting the dependence on foreign vendors or critical infrastructures outside sovereign territory. The privatisation of critical infrastructures and the increasing dependence on the cyber domain, however, has produced the complex interdependencies of modern information infrastructures and services to the point that this is not possible any longer. Whilst national governments try to manage such dependencies, it is proving too much of a moving target for the most. One principal reason for this is the attempt to address the problem within a context of a framework that is rapidly expiring:

[1] http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy.

> traditional categories of infrastructure do not adequately capture the complexity or speed of the modern ecosystem, and many countries depend increasingly on infrastructure and assets over which they have little or no control (Chatham House 2013: vi).

Other options to approach the problem, however, are not problem free either. One approach is to limit the scope to attempting to address the dependency on the global internet infrastructure by focusing on promoting global governance and international norms that match with national goals. The underlining assumption behind this approach is that cyberspace is public good or a global commons. Josepth S. Nye, however, disagrees and argues that "public good is one from which all benefit and none is excluded", whilst cyberspace is dependent on physical resources within the boundaries of sovereign states (Nye 2010: 15).

Nonetheless, international collaboration, regional and global governance is required in order to develop "rules of the game" in the form of international norms for ensuring the confidentiality integrity and availability of the global cyber domain and the privacy of the information passing through it. Currently Internet global internet governance is divided between different parts of the global infrastructure and between intergovernmental and non-governmental. A private sector non-profit organisation the Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for domain names and routing management. The Internet Engineering Task Force (IETF), on the other hand develops voluntary internet standards on transport, routing and security, but is best know for managing the TCP/IP protocol. The Internet Governance Forum (IGF) is a non-governmental organisation, acting as a multi-stakeholder forum for policy dialogue on internet governance. The IGF was established as a result of the World Summit on the Information Society (WSIS) meetings organised by the United Nations (UN) in 2003 and 2005. Finally, The World Wide Web Consortium is non-governmental organisation dedicated for development of standard for the world wide web, for instance by coordination to avoid incompatible versions of the HTML code.

The most influential intergovernmental organisation involved in global internet governance is the International Telecommunications Union (ITU). The ITU is a United Nations (UN) agency for ICT sector cooperation between the member states and the private sector. ITU promotes global collaboration in cyber security regulations and standardisation. This international division of labour reflects the vision of the internet as a commons and free from government interference.

However, considering that security is a traditional function of government, increasing insecurity may lead into increasing role for governments in cyberspace. In fact, many countries already desire to extend their sovereignty in cyberspace and are seeking technological means to do so. Whilst this could be taken as a sign of return of the state, Nye suggests that it may be true "…but not in the ways that suggest a return to traditional Westphalian paradigm of sovereignty" (Nye 2010: 15). Nonetheless, for instance China is focusing on building a strong domestic industry in order to have the ability to disconnect from the global internet and function on domestic resources behind the "Great Firewall" if deemed necessary. Russia is reportedly aiming at the same goal.

What seems to be unavoidable is the growing need of striking a balance between the benefits of open access to the global internet and the risks that may be associated with such reliance. When national security interests and the benefits of a free global internet are at conflict, the latter would seem to win. What government can do when this conflicts becomes unbearable is a question that is likely to penetrate the national security agenda in force in the future. There is increasing doubt whether nation-states have the tools to shape governance of the global internet so that it would both continue to produce the benefits to businesses and citizens, but also correspond better with national security interests. One major hurdle is that governments lack the competencies to solve this complex problem. Too much regulation hampers growth and the freedoms a free internet brings, but too little risks to incapacitate the government as a security actor. As a Chatham House report on the topic concludes:

> government policies can shape the landscape for better or worse, but there are no solutions that will satisfy all stakeholders, since they are shaped by the subjective perspectives and inevitably limited knowledge of decision-makers (Chatham House 2013: x).

Even if some sort of a balance between security and freedom would be found, the sheer scale of internet connected systems and services provides an enormous selection of “attack surfaces”. Coupled with the inherit complexity, this probably leads to decreasing ability to detect and respond to incidents. Hyper-connectivity brings more vulnerabilities that can be exploited, who takes responsibility for what, especially in the case when a critical infrastructure for country X resides in country Y and a service disruption puts critical services at risk in X? (Chatham House 2013: 8). Who is responsible for what in such a scenario? Countries could of course attempt to offer “opt in” incentives for private owners of critical infrastructure to join security (national) systems rather than rely on open internet or rely on infrastructures on foreign soils (Nye 2010: 17), but on what basis would the government choose the companies that are allowed to participate? Such incentives would offer a competitive advantage for a select few, on what basis would companies be excluded? If the idea is to support domestic companies, which companies would be considered as “domestic” and on what grounds? Based on a percentage of domestic ownership? What if a multinational or even a company owned by a foreign government offers services that are so critical it should qualify, would they nonetheless be excluded? The effectiveness of such opt ins would be highly doubtful in the long-run.

> Finally, one could of course continue to place belief in the robustness and resilience of the Internet. The best advice thus far for dealing with the risks of hyper-connectivity comes from Rod Beckstrom, who argued that the correct approach is based on three laws or assumptions: 1) Everything that is connected to the Internet can be hacked, 2) Everything is being connected to the Internet and, 3) Everything else follows from the first two laws. (WEF 2012: 10)

5 Establishing a Holistic Strategy for National Security in a Hyper-connected World

Given the constantly increasing dependence of a modern nation-state on global flows and networks for the resources and knowledge, such as goods, services, people and information required for the provision of the positive political goods to its citizens, it is justifiable to ask whether the traditional concept of national security is still valid? The global flows and networks providing the resources and the global commons, the seas, air, space and the cyber domain, that provide the required channels for them, reside outside the borders of the nation-state and thus, outside their realm of control. However, without a constant and stable access to these resources a nation-state will not be able to maintain a competitive national economy, nor increasingly, effective national security. Consequently, a successful modern nation-state needs to secure adequate access to these global flows in relation to its goals (which may vary from state to state depending on variety of particularities, e.g. political system and political culture), to fulfil the desires of its citizens that are manifested through a political process. In order to secure its access to global networks and flows, the governments will need to further link disparate policy realms, e.g. economic, security, defence and foreign policy, closer together into a holistic global strategy to secure its place in the global system.

However, it should be recognised that the global flows are resilient in their dynamics, in a sense that if a flow is disrupted in one domain, it simply finds an alternative route to reach its goal through a complex dynamics of push and pull factors. Take for an example the global flows of illegal immigration, international drugs trafficking or illegal finances. When one access route to a territory that offers sufficient pull (demand) is blocked or disrupted, the push (supply) will adjust and direct itself through other routes of access. Since, a nation-state is essentially a complex adaptive system itself, having born out of a process of constant redefinition and having evolved through wars and crises, flows of immigration and emigration, the only fundamental challenge is the traditional concept of territoriality that the nation-state has relied upon as a social structure. The global flows can be adjusted and redirected by nation-states through a number of policy controls, such as immigration and border protection, but they do not respect borders as physical constraints. This challenge, however, can be mitigated by adopting a new line of thinking regarding territoriality, which involves given up thinking of a nation-state as a “container” with clearly defined and solid borders and start thinking about it as more like a local network made up of a multitude of nodes and connections to a larger global network of networks. This would also suggest thinking about citizens and constituencies similarly as users are thought of in information networks, expecting certain service levels from the network operator. Consequently, the objective of the nation-state would be to manage the direction, intensity, content and dynamics of global flows to and from its territory to the benefit of its citizens. Hence, the strategic objective of a national security should be establishing robustness of the critical local nodes connected to the global flows and adaptability in terms of creating a capability to adapt its structures and resources to match the dynamic changes in global flows. In sum, in a hyper-connected world the emphasis should be the security and continuity of connectivity, instead of attempting to establish sovereign control over these dynamic and fluid processes and flows. A report by the Finnish Institute of International Affairs (FIIA) investigated the restrictions and opportunities for national preparedness in such a world, concluding that global interconnectedness and interdependency are likely to increase in importance in the national security agenda in Finland and elsewhere (Aaltola et al. 2014). A joint report by FIIA and the National Emergency Supply Agency (NESA) currently on the way aims to identify and analyse international dependencies that are important for Finland's critical societal functions and infrastructures, the threats and opportunities that relate to those and the propriety responses to them.

This in turn would have to be reflected in the concept of "criticality". It is simply not adequate to state that certain physical assets, such as international ports or airports are "critical", without defining what value they create for the society. This would require adopting a relative and dynamic concept of "criticality", in which criticality may vary in different temporal and spatial contexts and in relation to other critical services. For instance, a port or an airport can have different degrees of criticality depending on what critical resources are supposed to be passing through it at different time. Consequently, whilst it is increasingly difficult, prioritization is a must. The simple fact is that the focus of "critical infrastructure" keeps expanding, whilst not everything can be protected. As was pointed out in a Chatham House report on critical international dependencies, "when everything is 'critical', nothing is" (Chatham House 2013: iv). In fact, the report refuses to refer to "critical national infrastructure" on the basis that its definition has expanded so much that it is lost its usefulness. Moreover, one should consider the strengths and weaknesses of risk and resilience based approaches to "hyper risks". It would seem obvious that in a hyper-connected world threats are harder to anticipate, assess and mitigate, which would suggest that risk-based approaches will have decreasing utility, whilst resilience approaches may gather increasing importance. Moreover, the concept of security in the context of critical infrastructure is questionable in a reality where it is becoming impossible to define defensive parameters. In fact, such strategies will have little meaning when connectivity is valued above security (Chatham House 2013: 6). Strategies that aim to build adaptive capabilities could, however, be hampered by the fact that government decision-making (at least in democracies) is not equipped for real-time, or near-real-time, temporal scope. Responding to an event that takes places in seconds, could take hours, day, weeks or even months. On the other hand, managing long-term cascading risks is not necessarily a core capability of governments either due to the adverse effect of election cycles. The risk-based approach is more convenient for state security bureaucracies, however, as it is more easily aligned with planning and budgeting. In terms of closing the gap between internal and external aspects of security, national security policies must be aligned with foreign policy in a more integrated and holistic manner, as well as with trade and economic policies in general, in a similar manner that national economic policies have been linked to foreign policy. The mix of hard and soft security, could in this context mean combining security and continuity in a manner that guarantees an acceptable minimum at all times, whilst utilising adaptability capabilities to recover to "normal" fast and cost effectively. Cyber security is a good example of this, as it is impossible to establish perfect security in the cyberspace. In terms of managing international dependencies, it is clearly necessary to enhance the efforts concerning international norms and information sharing on incidents and best practices. Moreover, practical cooperation should be explored in novel ways, e.g. by establishing "trusted networks" or even "federated" systems for managing risk in critical information infrastructures that are so connected and networked that conventional approaches are bound to have little effect in any case. These could entail establishing bi- and multilateral Memorandums of Understanding or Mutual Assistance Agreements for the security and continuity of transnational and extra-sovereign critical commons. It could be also worth considering a CERT-network type arrangement for a broader CIP focus. In any case, we may be nearing a situation where the discussion between "infrastructure" and "information infrastructure" is pointless (Chatham House 2014: 17), as well as that between CIIP and cyber security, and it could be better to establish a concept that genuinely captures all these aspects.

As for the privatization of critical infrastructures, it should be noted that a conscious decision has (apparently) been made to trust critical infrastructures to be privately owned and operated because it has been determined that under "business as usual" conditions this ensures the best and most cost effective services to citizens. The realisation that markets may not be trusted to provide uninterrupted service in crises situations simply cannot be a surprise. There is no way the private sector could secure critical infrastructures against low probability—high impact risks, it is simply not economically viable. What must be determined is what magnitude of risk is acceptable, what is not and who then takes the responsibility. Nonetheless, it would seem that this reality is only now starting to sink into the consciousness of decision-makers. It should not be a shock that private sector is committed to provide public good to the extent they are paid to do so (Chatham House 2013: 28) and that their risk calculations are based on commercial logic. If societal risk is not communicated in a quantifiable manner and calculated into service pricing, why would it be a surprise when the robustness of critical infrastructure is perhaps less than perfect? The only way forward, which satisfies economic reality and national security is to determine the ownership and responsibility for risk gap that may exist between business risk and societal risk. This would have to entail determining who will close the gap, how and above all who pays for it?

Finally, at least some level of reevaluation concerning the relationship between sovereignty and national security in a hyper-connected world is unavoidable. Traditionally national security has been based on the notion put forward by Hans Morgenthau that national security depended on the ability of the nation-state to secure the integrity of its borders and institutions (Morhenthau 1960). In the hyper-connected world both have already been breached and the distinction will continue to erode. Consequently, the traditional concept of national security simply is not sustainable in the hyper-connected world. Given the low utility of Hobbesian thinking in strategically managing national security in such a world, perhaps it is time to cut the umbilical cord?

6 Conclusion

The future of national security in a world that is rapidly becoming "hyper-connected" cannot be based on dated models hailing back to thinking originating from the Peace of Westphalia in 1648. Whilst the nation-state and the concept of sovereignty are unlikely to be entirely abandoned, national security in the hyper-connected world cannot be locked in such absolute definitions of territorial sovereignty and dated understandings of critical infrastructures. Instead, novel approaches are required for functional national security in an emerging reality of dynamism and complexity where asymmetric threats increasingly cannot be identified, assessed and responded to utilising the traditional approaches, the answer may lay in a strategy that combines security and continuity and leverages on networked capabilities, instead of rigid national security bureaucracies. Finally, the concept "criticality" requires rethinking in such a world. Even now, not everything can be protected against anything, but when we lose the ability even determine what we should protect, against what and when, novel and more dynamic and relative concepts of criticality become a must. In sum, the emphasis should be the security and continuity of connectivity, instead of attempting to establish sovereign control over these dynamic and fluid processes and flows.

References

Aaltola M, Käpylä J, Mikkola M, Behr T (2014) Towards the geopolitics of flows: implications for finland. Available via FIIA. http://www.fiia.fi/en/publication/424/towards_the_geopolitics_of_flows/. Accessed 7 June 2015

Accenture (2015) Winning the industrial internet of things. Available via Accenture. http://newsroom.accenture.com/news/industrial-internet-of-things-will-boost-economic-growth-but-greater-government-and-business-action-needed-to-fulfill-its-potential-finds-accenture.htm. Accessed 26 May 2015

Australian Government (2010) Critical infrastructure resilience Strategy. Available via TISN. http://www.tisn.gov.au/documents/australian+government+s+critical+infrastructure+resilience+strategy.pdf. Accessed 28 May 2015

BBC News (2010) Wikileaks: site list reveals US sensitivities. Available via BBC. http://www.bbc.com/news/11932041. Accessed 30 May 2015

BlackRock (2014) Viewpoint. Available via BlackRock. https://www.blackrock.com/corporate/en-au/literature/whitepaper/viewpoint-us-equity-market-structure-april-2014.pdf. Accessed 27 May 2015

BlackRock (2015). http://www.blackrock.com/corporate/en-us/about-us. Accessed 27 May 2015

Buzan B (2007) What is national security in the age of globalization? Department of Foreign Affairs, Oslo. Available via Refleks. http://www.regjeringen.no/nb/dep/ud/kampanjer/refleks/innspill/sikkerhet/buzan.html?id¼493187. Accessed 3 July 2013

Chatham House (2013) Cyber Security and Global Interdependence: What is Critical?:6. Available via Chatham House. http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf. Accessed 29 May 2015, p 8

Chatham House (2014) Cyber Security and Global Interdependence: What is Critical? https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf. Accessed 2 June 2015

CNN (1997) Experts prepare for ‘an electronic Pearl Harbor’. Available via CNN. http://edition.cnn.com/US/9711/07/terrorism.infrastructure/. Accessed 26 May 2015

DHL (2014) Global Connectedness Index 2014. Available via DHL. http://www.dhl.com/content/dam/Campaigns/gci2014/downloads/dhl_gci_2014_study_high.pdf. Accessed 2 May 2015, p 8

Dillon M (2005) Global security in the 21st century: circulation, complexity and contingency. In: The globalisation of security, ISP/NSC Briefing Paper 2005/02, p 2

European Union (2008) Council directive 2008//114/EC. Available via Eur-Lex. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF. Accessed 30 May 2015

European Network and Information Security Agency (2012) European Cyber Security strategies. Available via ENISA. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper. Accessed 15 May 2015

European Commission (2013) Cybersecurity strategy of the European Union—an open, safe and secure cyberspace. Available via EC. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf. Accessed 26 May 2015

European Commission (2015) Critical Infrastructure. Available via EC. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm. Accessed 30 May 2015

European Union (2015) EU-US-Canada Expert Meeting on Critical Infrastructure Protection. Available via EU Newsroom. http://europa.eu/newsroom/calendar/events/2015/05/06_critical_infrastructure_protection_en.htm. Accessed 30 May 2015

Forbes (2013) Why we could easily have another flash crash. Available via Forbes. http://www.forbes.com/sites/deborahljacobs/2013/08/09/why-we-could-easily-have-another-flash-crash/. Accessed 27 May 2015

Government of Canada—Public Safety Canada (2015) Securing an open society: Canada’s National Security Policy. Available via Public Safety Canada. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/scrng-eng.aspx. Accessed 01 May 2015

Government of Canada (2015) Canada’s economic action plan. Available via http://actionplan.gc.ca/en/page/bbg-tpf/critical-infrastructure-and-cyber-security. Accessed 29 May 2015

Government of the Netherlands (2013) A secure Netherlands in a Secure world: international security strategy. Available via Government of the Netherlands. http://www.government.nl/documents-and-publications/notes/2013/06/21/international-security-strategy.html. Accessed 24 May 2014

Helbing D (2013) Globally networked risks and how to respond. Nature 497:51–59

Heng Y-K (2013) A global city in an age of global risks: Singapore’s evolving discourse on vulnerability. Contemporary Southeast Asia 35(3):423–446

HM Government (2010) A strong Britain in the age of uncertainty: the national security strategy. Available via HMG. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf. Accessed 28 March 2014

Investopedia (2014) High-frequency trading—HTF. http://www.investopedia.com/terms/h/high-frequency-trading.asp. Accessed 26 May 2015

Kahler M (2004) Economic security in the age of globalization: Definition and provision. The Pacific Review 17(4):485–502

Keohane RO, Nye JS (1977) Power and interdependence: world politics in transition. Little, Brown, Boston

Krause K (2007) National security in the age of globalization: a brainstorming note, Department of Foreign Affairs, Oslo. Available via Refleks. http://www.regjeringen.no/nb/dep/ud/kampanjer/refleks/innspill/sikkerhet/krause.html?id=493206. Accessed 3 July 2013

McKinsey Global Institute (MGI) (2013) Disruptive technologies: advances that will transform life, business and the global economy. Available via MGI. http://www.mckinsey.com/~/media/mckinsey/dotcom/insights%20and%20pubs/mgi/research/technology%20and%20innovation/disruptive%20technologies/mgi_disruptive_technologies_full_report_may2013.ashx. Accessed 26 May 2015. p 52

Milner H (2009) Power, interdependence, and Nonstate Actors in world politics: researchfrontiers. In: Milner H, Moravcsik A (2009) Power, interdependence, and nonstate actors in world politics. Princeton University Press, p 15

Moisio S, Paasi A (2013) Beyond state-centricity: geopolitics of changing state spaces. Geopolitics 18(2):255–266

Morhenthau HJ (1960) Politics among nations: the struggle for power and peace. Alfred A. Knopf, New York

Nanto D (2011) Economics and national security: issues and implications for U.S. policy. Congressional Research Service (CRS). Available via FAS. http://fas.org/sgp/crs/natsec/R41589.pdf. Accessed 27 May 2015

NATO Cooperative Cyber Defence Centre of Excellence (2015) Cyber definitions. Available via CCDCOE. https://ccdcoe.org/cyber-definitions.html. Accessed 5 June 2015

Neowin (2013) Microsoft: internet users will double to 4 billion worldwide by 2020. Available via Neowin. http://www.neowin.net/news/microsoft-internet-users-will-double-to-4-billion-worldwide-by-2020. Accessed 30 May 2015

Neu C.R, Wolf J. (1994) The economic dimensions of national security. RAND, Santa Monica. Available via RAND. http://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR466.pdf. Accessed 1 June 2015, p xi–xii

Nye J (2010) Cyber power. Available via Belfer Centre for Science and International Affairs, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf, Accessed 6 June 2015, p 15

OECD (2008) Protection of 'Critical Infrastructure' and the role of investment policies relating to national security. Available via OECD. http://www.oecd.org/daf/inv/investment-policy/40700392.pdf. Accessed 8 May 2013, p 3

Ripsman NM, Paul TV (2010) Globalization and the national security state. Oxford University Press, Oxford, p 10

Telecom Circle (2014) What is the internet of things? Available via Telecom Circle. http://www.telecomcircle.com/2014/05/what-is-internet-of-things/. Accessed 26 May 2015

The Economist Intelligence Unit (2014) The hypeconnected economy: how the growing interconnectedness of society is changing the landscape for business. Available via EUI: http://www.economistinsights.com/technology-innovation/analysis/hyperconnected-economy. Accessed 15 May 2015

The New York Times (2012) Panetta warns of dire threat of cyber attacks on U.S. Available via NY Times. Accessed 26 May 2015

UK Cabinet Office (2010) Strategic framework and policy statement on improving the resilience of critical infrastructure to disruption from natural hazards. Available via Cabinet Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf. Accessed 25 May 2015

Value Walk (2014) Goldman Projects "Internet of Things" to become biggest mega trend yet. http://www.valuewalk.com/2014/06/internet-of-things-to-become-biggest-mega-trend-yet/. Accessed 26 May 2015

We are Social (2015) Digital, social & mobile worldwide in 2015. Available via We are Social. http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/. Accessed 15 May 2015

Whitehouse (2012) National strategy for the global supply chain security. Available via Whitehouse. https://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf. Accessed 2 June 2015

Whitehouse, President Obama (2013) Cybersecurity. Available via Whitehouse. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity. Accessed 2 June 2015

World Economic Forum (2012) Risk and responsibility in a hyperconnected world. Available via World Economic Forum. http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience. Accessed 15 May 2015

World Economic Forum and Accenture (2013) Building resilience in supply chains. Available via WEF. http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf, p 7

Zurich, Atlantic Council (2014) Beyond data breaches: global interconnections of cyber risk. Available via Zurich. https://www.zurich.com/_/media/dbe/corporate/docs/whitepapers/risk-nexus-beyond-data-breaches-global-interconnections-of-cyber-risk%202014.pdf, p 14

Is Maritime Security a Traditional Security Challenge?

Ioannis Chapsos

Abstract This chapter discusses contemporary maritime security and examines the extent of its (non-)traditional nature in the context of international security. Based on the existing literature and adopted strategies, it highlights that there is no internationally accepted definition. Arguably, maritime security's concept depends on the perspective of the 'end user' and it broadens as far as the relevant stakeholders get involved. Still, contemporary maritime security is directly linked and interdependent with human security and development. The combination of human insecurity's non-traditional nature and the increasing involvement of non-state actors in projecting maritime insecurities, results in its differentiation from the traditional, interstate security challenges.

Keywords Maritime security · Maritime security strategy · Human security

1 Introduction

Maritime security increasingly draws international attention and sets the agenda for academics, policy makers and strategy planners, due to the high cost inflicted on the global economy and loss of human lives at sea. Modern piracy, terrorism, fisheries crime and smuggling of migrants by sea are only a few of the maritime insecurities which have made the headlines during the last decade. The research question that this chapter seeks to address is whether maritime security is a traditional security challenge or not, and where it fits in the context of contemporary international security.

For the purpose of this chapter, the author understands as traditional the realists' state-centric approach to security which aim to shift in the balance of power and

I. Chapsos (✉)
Maritime Security, Centre for Trust, Peace and Social Relations, Coventry University, Coventry, UK
e-mail: ioannis.chapsos@coventry.ac.uk

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_4

more specifically those security challenges which focus on military threats, stemming from interstate rivalries and disputes. As non-traditional, the author defines the threats which although stem from non-state actors' activities, they are highly transnational in nature, and challenge the state structure in social, political, economic and development terms. Still, although the two terms tend to be distinct, there are areas of overlap. Even more importantly, states have to address both of them and in order to implement efficient responses they have to develop appropriate security governance mechanisms, taking into account legal, jurisdictional and capacity issues, at the local, regional and international levels.

After reviewing the available definitions of maritime security in the existing academic literature, this chapter provides an overview of the developed and adopted maritime security strategies by international/regional/intergovernmental organisations' (African Union, European Union, NATO) and states' (UK, US) level.

It concludes that there is no internationally accepted definition and it depends on each 'end user's' perspective to broaden and deepen the approach and concept, based on its interests, focus, stakeholders involved and regional distinctiveness. However, all the analysis advocates that maritime security is mostly challenged by non-state actors, although the required responses at international level remain a responsibility of states and intergovernmental organisations.

In this framework, the chapter also highlights the nexus between maritime and human security. The former has severe direct and/or indirect implications on economic, food, social and energy securities, which are some of the latter's fundamental components. Still, human insecurity ashore undoubtedly emerges as the primary push factor for insecurities at sea. The perpetrators incline towards transnational organised crime rather than interstate violence, which to a great extent define maritime security's characteristics as a non-traditional challenge.

2 Defining Maritime Security

In the contemporary geopolitical environment, maritime security has emerged as one of the most significant elements of global and human security (Reveron and Mahoney-Norris 2011: 129–157). Through this, it contributes to economic development from the local to the regional up to the international levels. The sea-based trading system, developed mostly by littoral states, offers access to and distribution of energy resources, raw materials and all kind of products around the world. Hence, since almost 90 % of the global trade is transported in ships' hulls, littoral states developed maritime infrastructure in order to establish these energy supply chains and links between them and the hinterland and ensure the secure flow of goods to the international markets (Sakhuja 2010: 3–11).

There are a variety of possible definitions of maritime security, the form of which depends on the specific perspective taken. As an element of the broader concept of global security, maritime security was, and is, traditionally related to a state's military interests.

On the one hand, the vastness of the oceans provides huge ungoverned areas within the leaderless international system. These areas are outside any state's jurisdiction, the *mare liberum*,[1] providing a large part of the common goods. On the other hand, the littoral and coastal waters are directly related to a state's sovereignty, as well as projecting and enforcing power on other states. Hence, throughout history the oceans' role in military terms has been of great strategic importance, and their security cannot be taken for granted due to their size and the consequent 'tyranny of distance'. Moreover, oceans magnify the states' relative power by enabling global reach, competent seaborne trade, and control of territories, people, and vital offshore resources. Obviously, these factors also boost the state's development and economic sustainability, a role critical for achieving the desired circumstance of 'freedom from want and freedom from fear'.

Inevitably, all these advantages have also generated and motivated disputes between coastal states, due to efforts to claim jurisdiction over as large a sea-area as possible. In this framework, the definition of maritime security becomes rather complicated and multi-dimensional (Klein 2011: 130–133; Reveron and Mahoney-Norris 2011).

2.1 The Academic Approach

Within the broader conceptual debate on security, it is possible to identify maritime security as a specific dimension of global security, since all contemporary challenges of global security can also be applied to the maritime domain, such as for example "maritime environmental security" and "maritime terrorism", etc. Furthermore, the existing literature tends to focus on the sea and its characteristics as a means to a variety of uses, as well as on the seaborne threats to these same applications (Rahman 2009: 29).

Following the paradigm of many significant global issues lacking internationally accepted definitions, analogous efforts have been made within the academic community to define maritime security. These reflect the different perspectives involved in security, such as the professional domains in which it might be used, but they simultaneously entail a greater spectrum of contemporary threats.

For example, from the shipping industry aspect, maritime security could be defined as the avoidance of violence at sea which could encompass a broader reference to piracy, maritime terrorism etc., without the need to provide specific legal definitions for each crime. Moreover, from the shipping industry operators' perspective, maritime security focuses on transportation systems and the safe delivery of cargoes without violent interruptions. In this framework, Hawks defines maritime security as,

[1] Latin, meaning the 'freedom of the seas', as described in the Dutch philosopher and jurist Hugo Grotius' 1609 book, *Mare Liberum.*

> those measures employed by owners, operators, and administrators of vessels, port facilities offshore installations, and other marine organisations or establishments to protect ships against seizure, sabotage, piracy, pilferage, annoyance or surprise (Klein 2011: 8).

McNicholas (2008) analyses and highlights the threats in the maritime domain from a security-oriented perspective. He addresses issues such as port security, drug smuggling, piracy and maritime terrorism, and also provides recommendations for mitigation strategies. Thai (2009) argues that one of the fundamental questions relevant to this field is how effective maritime security can be achieved in practice, e.g. satisfying security requirements while enhancing other business objectives, such as service quality or operational efficiency. In other words, it is important to identify and comprehend the critical success factors (CSFs) for the effective management of security in maritime transport. Hence, he attempts to identify critical factors of effective maritime security and empirically evaluate them. After identifying the gap in the academic literature, he concludes that a conceptual model of effective security management in maritime transport is essential and lacking. He proposes, therefore, an effective maritime security model which consists of 13 dimensions and focuses on policy, strategy, governance issues and their implementation (Thai 2009: 147–148, 160).

Bueger (2015) utilised three different theories in order to answer the question 'what maritime security is': semiotics, securitisation and security practice. He confirms that there is no globally accepted definition resulting in the consequent implications and he approaches maritime security as a 'buzzword', which generates endless disagreements about what it might mean in practice (Bueger 2015: 159–60). However, in policy formulation, it allows for

> a measure of ambiguity to secure the endorsement of diverse potential actors and audiences, […and it provides…] concepts that can float free of concrete referents, to be filled with meaning by their users, […], shelter multiple agendas and provide room for manoeuvre and space for contestation (Bueger 2015: 160).

In this framework he introduces the matrix shown in Fig. 1, with four maritime security concepts and their potential relations, where different actors have to decide which of those fell under their interests, focus and priorities and develop/adopt the respective strategies and responses. Although this is a very comprehensive and holistic approach, which presents all the dimensions of the contested maritime security concept—including the human security dimension which will be discussed in the next section—he also sees marine safety and accidents as part of this matrix. By definition though, safety and security are quite distinct where the former refers to accidents and the latter to criminal activities. Even the UN Secretary General in his 2008 report to the General Assembly, under the title "Oceans and the law of the sea" made a clear distinction between the two terms (UN General Assembly 2008: 15, 44), providing the following definition for maritime safety:

> Maritime safety is principally concerned with ensuring safety of life at sea, safety of navigation, and the protection and preservation of the marine environment. The shipping industry has a predominant role in that regard and many conditions must be fulfilled before a vessel can be considered safe for navigation: vessels must be safely constructed, regularly

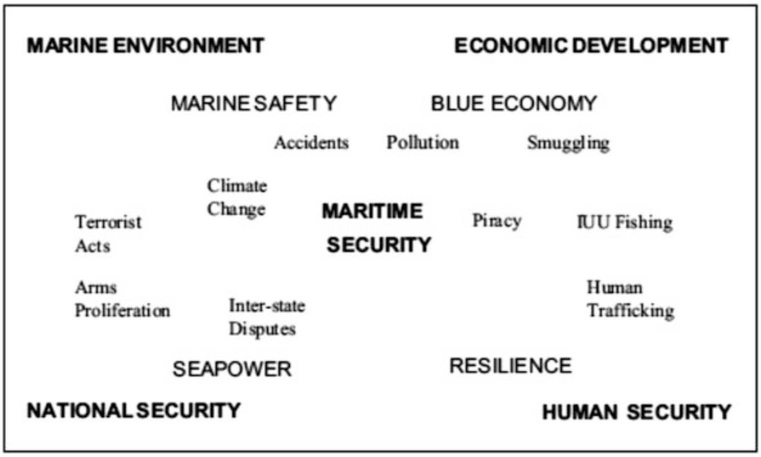


Fig. 1 Maritime security matrix. *Source* Bueger (2015: 161)

> surveyed, appropriately equipped (e.g., with nautical charts and publications) and adequately manned; crew must be well trained; cargo must be properly stowed; and an efficient communication system must be on board (UN General Assembly 2008: 44).

Consequently, and based on the above, this chapter argues that on the theoretical level maritime safety and accidents are quite distinct from maritime security issues. The EU Maritime Safety Agency[2] for example is characteristically distanced and abstained from any reference to security issues. On the contrary though, relevant state agencies (Coast Guards for example) in practice often have to deal with both safety and security issues. Hereof, although the reasoning behind this matrix is understandable, we need to keep the two domains with clearly defined boundaries and avoid overlapping which might cause confusions in policy making and strategy planning aiming at addressing maritime insecurities and criminal activities.

Bueger (2013, 2015: 163) finally introduces the concept of maritime security communities, which describes an advanced form of cooperation between all actors relevant to the maritime sector. In this form of cooperation, all maritime stakeholders need to jointly identify which threats exist in their environment, for which referent objects, and what should be done about it. The required actors to address them should engage on a day to day basis, share information and coordinate their activities. They also need to establish common understanding and tools to foster maritime security. He finally distinguishes the concept of security communities from other types of security governance in the sense that it focuses on identifying distinct threats and ways that a community could deal with them collectively, by primarily engaging lower and mid-level security practitioners and experts and the ways they should interact (Chapsos & Kitchen 2015: 2).

[2] See EU Maritime Safety Agency (EMSA), available from http://www.emsa.europa.eu/ [accessed May 2015].

3 International Organisations and States

The Secretary General of the United Nations in his 2008 report to the General Assembly, under the title “Oceans and the law of the sea” (UN General Assembly 2008) addressed maritime security. After making clear that there is no universally accepted definition, but that different versions and meanings are attributed to the term depending on the context and the user (UN General Assembly 2008: 15, para 38), he identified seven specific threats to maritime security:

> Piracy and armed robbery at sea; terrorist acts involving shipping; offshore installations and other maritime interests; illicit trafficking in arms and weapons of mass destruction; illicit traffic in narcotic drugs and psychotropic substances; smuggling and trafficking of persons by sea; illegal, unreported and unregulated fishing; and intentional and unlawful damage to the marine environment (UN General Assembly 2008: 17–33).

The UN Secretary General also refers to the ‘narrow conception’ of maritime security, which is conceptualised in state-centric terms, such as threatening territorial integrity with projections of naval power and use of force by naval assets. Yet, his report, as a whole, refers to a broadened human-centric approach that calls states towards a more collective maritime security and recognises that the new evolving threats go beyond the use of force and state boundaries, reflecting the human insecurity conditions ashore.

The increasing significance of maritime security in the context of international security and development, as well as its realisation from intergovernmental organisations, resulted in the development and adaptation of maritime security strategies from the African Union and the European Union in 2014.

The 2050 African Integrated Maritime (AIM) Strategy is inclusive and based on a human-centred approach to security and development where all social groups are engaged. It identifies the wide variety of related activities and the extent of their interconnectedness, as well as the potential impact on the prosperity derivative through their contributions to social, economic and political stability, safety and security (AU 2014: 7). The AIM strategy builds on the fundamental principles of the human security approach, meaning it aims both to address the root causes of insecurity and to improve the everyday lives of member states’ citizens (Chapsos 2014). In this framework, it highlights that the African maritime domain is challenged by the following threats:

- Transnational Organised Crimes in the maritime domain[3];
- Illegal, Unreported and Unregulated (IUU) Fishing, overfishing, and Environmental Crimes[4];
- Natural Disasters, Marine Environmental Degradation and climate change;

[3] Includes Money Laundering, Illegal Arms and Drug Traffic, Piracy and Armed Robbery at Sea, Illegal Oil bunkering/Crude Oil Theft along African coasts, Maritime Terrorism, Human Trafficking, Human Smuggling and Asylum Seekers Travelling by Sea.

[4] Includes deliberate shipwrecking and oil spillage as well as dumping of toxic wastes.

- Strategic Communications Systems;
- Vulnerable legal framework;
- Lack of and/or poorly maintained aids to navigation and modern hydrographic surveys, up-to-date nautical charts and maritime safety information in a number of AU Member States (AU 2014: 11).

In this context and without providing a specific maritime security definition—following the UN paradigm—it sets the strategic objectives to address the threats, which include the civil society's and all other stakeholders' engagement to improve awareness on maritime issues; enhancement of political will at community, national, regional and continental levels; enhancement of wealth creation, and regional and international trade performance through maritime-centric capacity and capability building; ensuring security and safety of maritime transportation systems; prevention of hostile and criminal acts at sea, and coordination/harmonization of the prosecution of the offenders, etc. (AU 2014: 12).

In a similar vein, the European Union (EU) adopted its maritime security strategy (EUMSS) in 2014, where it highlights the need for better sea border management. It refers to both internal and external aspects of the EUMSS aiming at providing

> …effective and cost-efficient responses to the protection of the maritime domain, including borders, ports and offshore installations, in order to secure sea borne trade, address potential threats from unlawful and illicit activities at sea, as well as to make optimal use of the sea's potential for growth and jobs, whilst safeguarding the marine environment (EU 2014: 1).

In this framework, maritime security

> is understood as a state of affairs of the global maritime domain, in which international law and national law are enforced, freedom of navigation is guaranteed and citizens, infrastructure, transport, the environment and marine resources are protected (EU 2014: 2).

The cross-sectoral approach, functional integrity, respect for rules and principles and maritime multilateralism have been utilised as the strategy's guideline principles (EU 2014: 3).

NATO's Alliance Maritime Strategy (AMS) 2011 identifies the four roles of NATO's maritime forces which are to provide deterrence and collective defence services, crisis management, cooperative security and maritime security (NATO 2011). Focusing specifically on maritime security, it entails among others the maintenance of the ability of NATO's maritime forces to undertake the full range of maritime interdiction missions, including in support of law enforcement and in preventing the transport and deployment of weapons of mass destruction. Concluding, it stresses that, achieving these requirements demand a high degree of coordination, interaction and training as well as a quest for complementarity whenever appropriate. In this context, it suggests that specific emphasis should be placed on standardising operating procedures, as well as on promoting joint exercises and training exchanges. It finally identifies the need to refine organisational structures, operational concepts, doctrine, training and education.

At the states' level, the UK national strategy for maritime security defines maritime security as:

> the advancement and protection of the UK's national interests, at home and abroad, through the active management of risks and opportunities in and from the maritime domain, in order to strengthen and extend the UK's prosperity, security and resilience and to help shape a stable world (UK 2014: 15).

Similarly, the US approach highlights that:

> maritime security protects U.S. sovereignty and maritime resources, supports free and open seaborne commerce, and counters weapons proliferation, terrorism, transnational crime, piracy, illegal exploitation of the maritime environment, and unlawful seaborne immigration (US 2015: 26).

The US strategy puts emphasis on both the navy's and coast guard's contribution in a robust maritime security provision, maritime domain awareness, and effective maritime governance, while defining their areas of jurisdiction respectively (ibid).

4 Maritime Insecurities: Actors Involved and the Causal Factors

Having analysed the available definitions of maritime security, as developed and introduced by academia, international and regional intergovernmental organisations and states, we realise the plethora and diversity of approaches based on the aspect of the 'end user'. Although there is no globally accepted definition for the same reason, we can definitely see common areas and traits in all approaches which will be utilised to gain a better understanding on maritime security.

First, contemporary threats to maritime security are well mapped, to a great extent interconnected, interdependent and interrelated, and to this end, the existing definitions are complementary to each other, rather than conflicting. None of the identified maritime security threats can be overlooked and no single actor—be it a single state or organization—can afford to exclude or downgrade the risk posed from each individual challenge. Still, there is an undeniable need to prioritise the significance, implications and required responses to each threat, based on the local and regional distinctiveness, local knowledge and interests.

Second, and based on the discussed maritime security matrix (Fig. 1) each actor must identify whether the whole spectrum of the four maritime security concepts and their potential relations fall under their interests, focus and priorities or limit them accordingly to be properly tailored and fit in their needs. This will consequently also result in an efficient management of assets and required resources to efficiently and sufficiently address them.

Third, on the national level, the provision of maritime security is a major inter-agency challenge, where all the involved stakeholders need to jointly identify and comprehend the critical success factors (CSFs) to efficiently and sufficiently address it. The broader the understanding and definition of maritime security, the wider the range of actors and stakeholders involved. While the precise form of national coordination, joint policies and operations, and information sharing depends on the design of governmental activity, different functional agencies require coordination. This includes civil-military coordination, and involves several governmental entities and ministries, as well as legal and law enforcement agencies, both on land and at sea. Still, it also entails the private sector's involvement and coordination, ranging from the fishing and shipping to the private maritime security industries (Bueger 2015: 163).

Given the strategic, political, economic and military significance that maritime security entails, Kerr (2010: 16) argues that the responsibility for its robustness primarily lies with governments and international bodies. The main government services for example involved in maritime security are police, coastguards, customs and naval forces. However, in maritime insecurity hot-spots, applied measures and security provision demand more resources than those available from these two main actors.

Inevitably, maritime security is also widely understood as a transnational task, hence regional cooperation is essential in terms of information sharing, shared responsibility and collective security, multilateralism and joint coordinated responses. This is consequential, given that maritime security threats are transnational and perpetrators operate across boundaries. Hence, maritime insecurity has transnational consequences due to the non-tangible nature of maritime territorial boundaries, and the complex transnational character of global shipping and trade in which any single operation includes various nationals and jurisdictions.

Mugridge (2009) looked at the behaviour and methodology of those perpetrating maritime crimes and challenge maritime security. He argues that they are localised, small in number, disparate and irregular; all of these traits make them closely aligned with those of the insurgents, who actually challenge the traditional governmental forces and agencies. He concludes that instead of deploying conventional forces against them, a multi-agency international response would be efficient and cost-effective. Maritime security is already identified as a multidimensional problem, which realistically and practically cannot be addressed in long terms by a solely military solution. Hence, in the framework of a co-ordinated and integrated response, and the required formulation of long-term plans at the states' level, his suggested actions and tactics include the neutralisation of criminals and terrorists and their separation from their support (Mugridge 2009: 308–309).

A brief overview of the three more indicative threats for maritime security that follows, in particular maritime piracy, terrorism and fisheries crime, will reflect all the above distinctiveness of the actors competing in the maritime domain.

4.1 Maritime Piracy

The nature and objectives of piracy have not changed throughout the ages and undoubtedly financial profit is the perpetual pull factor. The causal factors remain the same: the vast and lawless space of the sea (limitations and existing gaps in the UNCLOS's approach to piracy, as well as the state's sovereignty issues); favourable geography[5] (which combines rewarding 'hunting grounds', moderate levels of risk and proximate safe havens); weak or compliant states that provide safe havens and sanctuaries; corrupted elites that can protect and get benefits from piracy; and economic disruptions that open markets for plundered goods. In all its forms, regardless the region and throughout history, maritime piracy's root causes and causal factors have very minor differences and they all stem from state fragility ashore and inefficient governance (Murphy 2009: 21, 29–30).

On the one hand, state fragility—and especially in post-conflict environments—results in inability to efficiently enforce the law ashore, which is further deteriorated by lack of resources and training of the relevant agencies. On the other hand, piracy is a land-based activity, and its primary enabling factor is a land 'base' to ensure proper support, logistics and freedom of movement. Hence, fragile states offer through 'ungoverned spaces' an ideal environment for pirates' safe havens, which are throughout the history their sanctuaries, replenishment bases and starting point for either their plundered goods in various black markets, or laundering of ransom money. This also leads to the successful and secure establishment of the required transnational organised crime networks, which will both supply the pirate groups with the required equipment, fuel, weapons, etc., and siphon their 'profits' to other markets. This also partially explains why for example the skiffs used for pirate activities are also used to smuggle humans, drugs or weapons (Murphy 2009: 162–170).

Piracy by definition poses a threat to seafarers; however, based on this evidence, we can argue that local communities which coexist with pirate groups and the collateral transnational organised crime networks equally face insecurities which put them at high risk. Still, these usually marginalised, politically and socially excluded communities also face the dilemma stemming from the income reward, especially due to their insecure, post conflict environment. Alas, the income generated from the criminal activities is far more assuring in terms of improving their

[5] Piracy traditionally occurs close to coasts or in narrow seas (straits). It is clearly land-based and concentrated in areas such as the Caribbean, the Gulf of Aden (Somalia), the South China Sea, the Gulf of Bengal and the Gulf of Guinea (off Nigeria). In these areas, vessels are forced to move closer to the coast for both navigational and commercial reasons, offering the ideal prey for the pirates. Furthermore, they are more crowded, hence the resultant slower movement of the ships offers more targets that are easier to approach and board (Murphy 2009: 29–30; Murphy and International Institute for Strategic Studies 2007: 14).

everyday living conditions compared to the opportunities provided by their state. Hence, the ‘clan-based’ model of piracy is very common in all hot spots worldwide (Murphy 2009: 162–170; Mayr-Harting 2012: 29–45, 13–18) and illegality is a minor issue for those facing hunger, poverty and exclusion.

4.2 Maritime Terrorism

Shipping, offshore installations, ports and other maritime interests could be potential targets for terrorist attacks. Such attacks could have widespread effects and thus constitute a major threat to maritime security. According to the RAND Database of Worldwide Terrorism Incidents, the attacks related to the maritime domain represent only 2 % of overall attacks perpetrated since 1972 (RAND 2012). Yet, maritime terrorism includes a variety of threats and complicated scenarios, which pose significant challenges to global security.

Significantly, through its former leader, Osama bin Laden, Al Qaeda declared its vision of creating, ‘a greater state of Islam … established from the ocean to the ocean’ (Rawley 2011: 5). Its maritime ‘strategy’ included the ambition to have attacks against seaborne targets that would damage Western prestige and economy. Indeed, the terrorist attacks against the destroyer USS Cole[6] in 2000, and the French oil-tanker Limburg[7] in 2004, both in Yemen, confirmed these plans and reminded policy makers and security officials that, besides land and air, terrorist organizations can also attack seaborne targets (Luft and Korin 2004: 62).

Moreover, the terrorist attacks against Mumbai in 2008[8] demonstrated that the sea can also be used as the medium to launch well organised lethal attacks against targets ashore (Basrur et al. 2009). Maritime terrorism includes the proliferation of weapons of mass destruction (WMD), exploiting cargo ships and trade routes as the ‘delivery system’, or even using the ship itself as a WMD, following the paradigm of the 9/11 attack (Nincic 2005: 624–631).

Again, in all the above cases non-state actors are the perpetrators. Although their goals are political gains, in contrast with the financial motivation of piracy, the concept of maritime terrorism strongly inclines towards the irregularity of non-traditional threats, following the paradigm of the land based equivalent.

[6] Al Qaeda suicide bombers in a speedboat packed with explosives blew in the side of USS Cole, killing 17 sailors, in October 2000 in the Yemeni port of Aden. See BBC *On this day* (12 Oct), available from http://news.bbc.co.uk/onthisday/hi/dates/stories/october/12/newsid_4252000/4252400.stm [accessed May 2015].

[7] See BBC News (2002).

[8] See BBC News (2009).

4.3 Illegal, Unreported and Unregulated (IUU) Fishing and Fisheries Crime

Food insecurity has been identified as one of the major threats to international peace and security (UN 2004). In the context of the fishing sector, overexploitation of fishery resources remains a major challenge to achieving sustainable fisheries, and thus contributes to food insecurity around the world. It is well recognised that one of the main causes of overfishing is Illegal, Unreported and Unregulated (IUU) fishing. These fishing activities involve complex webs of actions and entities (Committee on Fisheries 2007), which have undermined international conservation and management efforts.

The 2050 AIM strategy for example indicatively highlights the significance of fisheries for local populations: whilst over 46 % of Africans live in absolute poverty—a figure that is still rising—fish makes a vital contribution to the food and nutritional security of over 200 million Africans and provides income for over 10 million (AU 2014: 8). Not surprisingly, IUU fishing holds a prominent role throughout the strategy, while fisheries and aquaculture industry, as well as fisheries' focused education and scientific research, are mapped within Africa's maritime sector's stakeholders and related areas of capacity building respectively (AU 2014: 13).

IUU fishing is another challenge which highlights the transnational and cross-boundary nature of maritime insecurity, irrespectively of states' sovereign territories, since it has been reported in many different regions and in international waters and zones under littoral states' jurisdiction. Furthermore, and on several occasions it has established links with organised crime networks and activities; a precondition for the perpetrators is to remain 'under the radar' and use the fishing industry as a legitimate business cover for their illicit activities. This complexity and multidimensionality of maritime security in general and crime in the fishing industry in particular, is highlighted in a comprehensive study where the UN Office on Drugs and Crime (UNODC) examined and reported criminal activities in the fishing industry (UNODC 2011). It exposed the extent of forced labour and abuse in the fishing industry, where both children and fishermen are trafficked by organised crime networks. In parallel, these networks are involved with illegal fishing—both in terms of their practices and focus on endangered species—'laundering' illegal catches in the international fisheries market, which can be achieved only with fraud documents, transhipments and corruption. As if this was not enough, it also reveals that in most of the cases, these organised crime networks exploit the fishing industry operators' skills and knowledge of the maritime domain and recruit them in order to expand their illicit activities. Hence, fishing vessels are most often used as the legitimate business cover to facilitate smuggling of migrants, and trafficking of drugs and weapons.

The discussed findings lead us to the obvious but required distinction between IUU fishing and fisheries crime. Although the two have a conceptual correlation and interconnection by default, they are distinct by scope and nature: the former mainly entails fisheries management issues such as the extraction of marine living resources and falls with the focus of the Food and Agriculture Organization (FAO). The latter though, as discussed earlier, includes a whole range of criminal offences, such as document fraud, trafficking and smuggling related crimes, money laundering, etc., mainly perpetrated by organised crime networks, hence falls under the mandate of the UNODC (Palma-Robles 2014). Again, as already discussed in detail with regards to the definition of maritime security, fisheries crime lacks an accepted legal definition. Thus, fisheries crimes can be defined as

> …those criminal offences defined as such in domestic law (including, but not limited to, such offences in marine living resources acts) committed within the fisheries sector, with the 'fisheries sector' referring to the entire value chain from vessel registration to sale (Witbooi 2015: 43–44).

Another enabling factor for this challenge too, is again coastal states'—and even more developing states'—inefficient and insufficient monitoring, control and surveillance of fishing activities, even over vessels flying their flag. This already difficult task of addressing IUU fishing becomes even more complicated due to the practice of numerous fishing vessels registered with countries other than the country of ownership, commonly known as Flags of Convenience (FOCs—or open registries). As the International Transport Workers' Federation (ITF) reports,[9] ship owners are encouraged to register their vessels in FOCs by cheap registration fees, low or no taxes, and freedom to employ cheap labour. Some FOCs have poor safety and training standards and no limitations in terms of the crew's nationalities, which from a security perspective creates a security gap. Thus, more effective flag states' and port states' control, as well as market-related measures, could significantly contribute to eliminating the phenomenon.

Many analysts also identify IUU fishing as the root cause of piracy in the Horn of Africa (Onuoha 2009: 41; Kisiangani 2010: 362). Foreign fleets that take advantage of the lack of governance ashore are leveraged in illegal fishing up to over-exploitation levels[10] and are also involved in the dumping of toxic waste in Somali territorial waters (Ama Osei-Tutu 2011). Although it is debateable whether IUU fishing is THE root cause of Somali piracy or not, it definitely played a significant role in developing the Indian Ocean's modern piracy model. Hence, these dual iniquities illustrate how interrelated maritime security challenges are. They also highlight the extent of maritime insecurities' non-traditional nature,

[9] See International Transport Workers' Federation (ITF), 'Defining FOCs and the problems they pose', available online from http://www.itfseafarers.org/defining-focs.cfm [accessed April 2015].

[10] "It is estimated that annually between $4–9 billion is generated from this illegal activity with encroachment in Sub-Saharan Africa's waters amounting to about $1 billion. With no effective authority over the territorial waters of Somalia, these fishing fleets have taken control of the 3300 km coastline available to Somalia and its abundant marine resources. It is estimated that annually about 700 international vessels illegally poach in Somali territorial waters exploiting species of high value such as deep-water shrimps, lobsters, tuna and sharks" (Ama Osei-Tutu 2011: 10).

increasing interdependence with transnational organised crime networks and direct links to human insecurities, as the following section will discuss in detail.

5 Exploring the Human and Maritime Security Nexus

On June 1st 1941, when USA were on the threshold of the Second World War (WWII), Franklin D. Roosevelt addressed the Congress in an effort to abolish the United States' isolationism, convince public opinion of the need to support the European allied forces, and demonstrate the gravity of the situation and the threat to global security.[11] In his speech, still famous as the "four freedoms speech", he identified four essential human freedoms that the world should be founded upon: the freedom of speech and of expression, the freedom of religion, the freedom of want and the freedom from fear (Roosevelt 1941: 7–8).

More than 50 years later, the 1994 UN Development Programme's (UNDP 1994) influential report claimed that the focus on the Cold War in state security 'had obscured and ignored the far more urgent security needs of the millions for whom security symbolised protection from the threat of disease, hunger, unemployment, crime, social conflict, political repression and environmental hazards' (Dannreuther 2007: 1). Thus, although conflicts still exist, mostly in a form of intrastate violence, there exists a plethora of other non-military threats in parallel, which need attention. These include issues such as 'the threat of environmental degradation, economic disparities and chronic poverty, diseases such as HIV/Aids, transnational crime, and international migration' (Dannreuther 2007: 1).

Hence, the concept of human security was developed from Roosevelt's 'four freedoms', with a primary focus on the standards of everyday living, human dignity, freedom, equality, justice and safety from diachronic threats such as lack of food, medicine, poverty and the nefarious constraints that affect everyday life (UNDP 1994). This concept demonstrates a metamorphosis of the contemporary international security landscape, although none of the threats that it focuses on is new. As there was a sharp decline in interstate conflicts in the post-Cold War era other threats which challenge international security at all levels emerged. Human security introduces a shift from the traditional state centric into the non-traditional human centric approach to security, where non-state actors have an increasing involvement in security issues. Still, security remains a responsibility of the state, which in turn has to address non-traditional security challenges, and the military means are not panacea to counter them.

[11] The whole story and the full text of the speech are available online from the Franklin D. Roosevelt Presidential Library and Museum; see http://www.fdrlibrary.marist.edu/fourfreedoms [accessed 10 March 2015].

‘Want’ can be interpreted as extreme, life-threatening poverty, where basic requirements such as nutrition and shelter are lacking. ‘Fear’ suggests vulnerability to sudden threats, which may range from political violence and armed conflict to natural disaster and epidemics. ‘Dignity’ implies that individuals and communities not suffer from exclusion and repression: they should enjoy full participation in political life, with freedom of expression and religion. These threats can be either direct or indirect, and not always life threatening, but they could be constitutive elements of vulnerability, leading to possibly wide-scale human welfare failures (Hunter 2013: 23). Hence, this new concept of global security is directly interdependent with development. Although we are not as yet able to explain precisely how they interact, parameters of socioeconomic development such as inequality, low growth, unemployment and weak economic institutions increase the risks of violence (World Bank 2010: 7).

It is difficult to ascertain if security provision is a paradigm that fosters development, or vice versa. But no one can deny that lack of development and insecurity goes hand in hand (Kaldor 2007: 182–197). Following from this contemporary perception of security, the ‘ethnic security dilemma’ emerged (distinguished from the traditional interstate security dilemmas). This involves modes of physical security; such as political, economic, social, cultural and environmental security (Wolff 2006: 76), the right to claim democracy, equality in terms of citizenship opportunities, just public policy, non-discrimination and fair distribution of social and economic goods (Nagel 2005: 127).

Almost sixty per cent of the earth’s population lives within 100 km from a coastline, demonstrating the great significance of the sea for humanity. As Bueger (2015: 161) stresses though, human security has several maritime dimensions, which range from the security of vulnerable coastal communities to the crews of vessels transiting high risk areas.

Focusing for example on fisheries, we realise how vital they are in terms of both source of food and employment for coastal communities around the world. Hereof, illegal (IUU) fishing threatens their own existence and directly affects their nutrition and wealth. Both food and economic security are challenged, inevitably and directly affecting their ‘want’ and consequently their human security. Similarly, IUU fishing endangers their marine environment, while indirectly encompasses ‘fear and dignity’ issues with cases of transnational crime, human smuggling,[12] slavery,[13] forced labour[14] and violence reported in the fishing industry. Similarly, the disruption of sea lanes due to maritime piracy has severe consequences in the transportation of raw material, oil and all other kinds of products, with obvious and direct implications in economic security and development. Inevitably, there are also

[12] See for example BBC News (2015).

[13] See for example Fox News (2015).

[14] See for example AlJazeera (2015).

implications in energy security for states dependant on oil imports and in food security accordingly. Hence, the combination of direct and indirect implications of maritime security in both human security and development, reveal the underlying mechanisms which provide the inseparable links between them.

Finally, one could argue that the lack of human security ashore acts as a motive for individuals to become involved in maritime crime, looking for better living conditions and survival. For example, the increasing ‘want, fear and indignity’ in coastal communities and the lack of proper infrastructure to provide them sustainable livelihoods, will very likely lead them towards maritime criminal/illegal activities to support their needs, as analysed earlier in the case of maritime piracy. They will seek for alternatives which will provide their families with the means to survive, and the dilemma whether they should perpetrate illegal activities or not doesn’t make sense, since their lives are threatened by poverty, malnutrition and indignity. Furthermore, the potential lack of robust law enforcement and efficient (maritime) governance could further motivate them towards criminal activities, providing them with ungoverned spaces transformed into safe havens and maritime crime sanctuaries.

Beyond the criminal dimension though, lack of human insecurity is definitely a push factor for irregular migration, which is very often seen by those who flee from insecure and underdeveloped regions as their only alternative to crime. It is beyond any doubt that people who live in (post-) conflict environments, places with high levels of violence, in extreme poverty, hunger, exclusion and perpetually experience ‘want, fear and indignity’ are most likely to seek for a better future for their families in other countries. Hence, human insecurity is the primary—if not the most important—push factor, which fuels migration.

Mugridge (2009) builds on credible evidence to suggest that in many states, maritime security lacks financial or political resources, sustainability, relevance or multi-agency coherence. He argues that the oceans still offer a relatively unregulated environment for non-state actors (such as non-state terrorists and transnational criminals) to successfully challenge world order and international security, with significant damage inflicted. Hence, he introduces the term “Sea-Blindness” as a

> … socio-political failure to acknowledge or recognise the importance of the maritime domain to both society and economies. This alien condition transcends society from politicians to the working citizen, from private industry to political bodies. The future physical and economic security of many nations depends upon the freedom to use the world’s oceans and their ability to potentially influence worldwide political events by military means (Mugridge 2009: 306).

He finally concludes that the field of maritime security provides fertile ground for further research; particularly in terms of threat analysis of the irregular, non-state actors involved. His work anticipates that such research will inform the growing debate over international maritime susceptibility and introduce new approaches to overcome the hitherto drawbacks and fill the existing security gaps, towards an effective maritime security regime (Mugridge 2009: 305–310). Clearly, all maritime security strategies discussed in the previous sections, require redirection towards international collaboration and identification of maritime security's non-traditional nature.

6 Conclusion

Maritime security is a contemporary multidimensional security challenge, which entails several threats (such as maritime piracy, human trafficking, smuggling, etc.) that challenge international security. However, their metamorphosis in their contemporary form and in the globalised marine environment, results in the proliferation and increasing involvement of non-state actors in maritime security issues and inevitably in transnational organised crime activities. In this framework, the lack of an internationally accepted definition demonstrates maritime security's multi-disciplinary nature but also the broad spectrum of the involved stakeholders. The analysis of the existing and adopted maritime security strategies provides concrete evidence for both the above conclusions. Each one of these strategies conceptualises and approaches maritime security from a distinct lens, based on local/regional distinctiveness, prioritisation of interests and the significance of each threat in their own context. Although most of the mapped maritime security threats have a place in all the reviewed strategies, their prioritisation is different. Each actor includes more (or less) threats, broadens and deepens the contested concept according to his own risk assessment, involved actors and emerging threats. In this context, the EU for example identifies 'Illegal and unregulated archaeological research and pillage of archaeological objects' (EU 2014: 8) as a maritime security risk and threat, while the UK introduced cyber-attacks against infrastructure and shipping (UK 2014: 19) in its list of threats.

As already discussed, the UN Secretary General urged states to broaden their approach to maritime security from the state-centric 'narrow conception' to a human-centric approach. He stressed that new evolving threats go beyond the use of force and state boundaries, reflecting the human insecurity conditions ashore; these cannot be addressed through the traditional means such as projections of naval power and use of force by naval assets, therefore a more collective maritime security response is required (UN General Assembly 2008). The human security concept eventually influenced strategy planners and the AU AIM strategy for example heavily builds on it. Still, there are elements of the traditional territorial disputes and naval force projection approach in almost all the adopted strategies. The AU for example calls upon member states to resolve existing maritime boundary issues and claim their respective maritime limits and their extended continental shelf (AU 2014: 22). The EU sees a possibility for the threat of use of force against member states' rights and jurisdiction over their maritime zones in its list of maritime security risks (EU 2014: 7). The UK identifies potential disruption to vital maritime trade routes as a result of war (UK 2014: 19), and among its primary objectives it focuses on protecting the UK and Overseas territories, citizens and economies (UK 2014: 18), in order to protect and advance its national interests at home and abroad. The US approaches maritime security as the protection of its sovereignty and maritime resources (US 2015: 26). Through these strategies, we can see a 'dual' approach to maritime security; a combination of the traditional state-centric character of threats to sovereignty and defence through military means alongside non-traditional threats such as irregular migration and illegal fishing. It is also evident that there is a shift in the traditional tasks of military forces in general and naval assets in particular, increasingly engaged with constabulary roles in the world oceans and 'common goods'. This paradox, having military forces, the traditional force projection and security provision actors, engaged with non-traditional threats highlights the complexity of maritime insecurities in the context of international security, as well as the diversity of involved state and non-state actors.

Maritime security has a traditional dimension too. Territorial disputes for example in the South China Sea (Glaser 2012; Kaplan 2011) demonstrate the inter-state rivalries with international consequences, which urge strategy planners not to overlook this potential in their developed strategies. There are also cases where state actors generate maritime insecurities, such as in the case of Libya (Chapsos 2015). Still, even in this case, state fragility and intra-state rivalries appears to be the root cause. Limited law enforcement capabilities ashore allow transnational organised crime networks to flourish and extend the insecurity at sea, in the form of human smuggling, trafficking, etc., with severe implications in regional and international security.

The international community is evidently challenged by maritime insecurities in multiple dimensions. State and non-state actors are involved and amalgamated both as potential perpetrators and security providers and the distinction between them becomes increasingly blurred. Traditional security challenges are at least clear in the sense that one state actor claims, for example, a territory or marine zone which under the existing status belongs to another state actor, and the international community to a great extent developed mechanisms to try and resolve them. Yet, things are far more complicated when it comes to non-traditional security challenges, as this chapter discussed about maritime security. Transnational criminal networks and terrorist groups have quite different objectives and goals and cannot be addressed through the mechanisms and maritime security governance structure developed for use by state actors only.

Still, state actors and in particular the military, are mostly involved in short to medium term responses, and up to the operational level. At the strategic level though, and looking for long term responses which will address the root causes, human security seems to be the required approach to form proactive policies and strategies to minimise the push factors ashore. The genesis, development, sustainability and spill over of maritime insecurities occurs on land, hence it is more effective and efficient to address them as land based crimes, rather than looking for reactive responses at sea.

References

AlJazeera (2013) Forced labour on Thai fishing boats, May 29. Available from http://www.aljazeera.com/video/asia-pacific/2013/05/20135293350699702.html. Accessed May 2015

Ama Osei-Tutu J (2011) The root causes of the Somali Piracy. Kofi Annan International Peacekeeping Training Centre KAIPTC Occasional Paper No. 31

UN General Assembly (2008) Oceans and the law of the seas. Report of the Secretary General, A/63/63

AU [African Union] (2014) 2050 Africa's integrated maritime (AIM) strategy. Available via AU. http://pages.au.int/maritime/documents/2050-aim-strategy-0. Accessed Mar 2015

Basrur R, Hoyt T, Rifaat H, Mandal S (2009) The 2008 Mumbai terrorist attacks: strategic fallout. In: S. Rajaratnam (ed) RSIS monograph No. 17. School of International Studies, Singapore

BBC News (2002) Yemen says tanker blast was terrorism, 16 Oct 2002. Available online from http://news.bbc.co.uk/1/hi/world/middle_east/2334865.stm. Accessed May 2015

BBC News (2009) Mumbai attacks: key sites, 26 Nov 2009. Available online from: http://news.bbc.co.uk/1/hi/world/south_asia/7751876.stm. Accessed May 2015

BBC News (2015) Rohingya migrants' boat rescued off Indonesia, May 11. Available from http://www.bbc.co.uk/news/world-asia-32680911. Accessed May 2015

Bueger C (2013) Communities of security practice at work? The emerging African Maritime Security Regime. Afr Secur 6(3–4):297–316

Bueger C (2015) What is maritime security? Mar Policy 53:159–164

Chapsos I (2014) Africa's plan to police violent seas is more hope than strategy. Available via the conversation. https://theconversation.com/africas-plan-to-police-violent-seas-is-more-hope-than-strategy-23220. Accessed May 2015

Chapsos I (2015) How chaos in Libya spawned a security nightmare in the Mediterranean. Available via the conversation. https://theconversation.com/how-chaos-in-libya-spawned-a-security-nightmare-in-the-mediterranean-41478. Accessed May 2015

Chapsos I and Kitchen C (eds) (2015) Strengthening maritime security through cooperation. NATO Science for Peace and Security Series, E: Human and Societal Dynamics, 122, Amsterdam: IOS Press

Committee on Fisheries (2007) Combatting illegal, unreported and unregulated fishing through monitoring, control and surveillance. Port State measures and other means. COFI/2007/7, Twenty-seventh Session edn., translated by FAO

Dannreuther R (2007) International security: the contemporary agenda. Polity, Cambridge

EU [European Union] (2014) European Union maritime security strategy, 11205/14. Available via EU. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT. Accessed Mar 2015

Fox News (2015) Migration agency: 4,000 fishermen, many slaves, stranded on Indonesia islands AP investigated, Mar 27. Available from http://www.foxnews.com/world/2015/03/27/migration-agency-4000-fishermen-many-slaves-stranded-on-indonesia-islands-ap/. Accessed May 2015

Glaser BS (2012) Armed clash in the South China Sea. Available via Council on Foreign Relations. http://www.cfr.org/world/armed-clash-south-china-sea/p27883. Accessed May 2015

Hunter A (2013) Human security challenges. We Leen editions, CPRS Books/eBooks Series No. 1

Kaldor M (2007) Human security. Polity Press, Cambridge

Kaplan RD (2011) The South China Sea is the future of conflict. Available via foreign policy. http://foreignpolicy.com/2011/08/15/the-south-china-sea-is-the-future-of-conflict/. Accessed May 2015

Kerr G (2010) Maritime security and the private security perspective. J Int Peace Oper 6(2):15–16

Kisiangani E (2010) Somali pirates: villains or victims? S Afr J Int Aff 17(3):361–374

Klein N (2011) Maritime security and the law of the sea. Oxford monographs in international law. Oxford University Press, Oxford

Luft G, Korin A (2004) Terrorism goes to sea. Foreign Aff 83(6):61–71

Mayr-Harting T (2012) Statement on behalf of the European Union by H.E. Mr. Thomas Mayr-Harting, Head of the Delegation of the European Union to the United Nations, at the Security Council Open Debate on the situation in Somalia, European Commission, New York. Available via Relief Web. http://reliefweb.int/report/somalia/eu-statement-united-nations-security-council-situation-somalia. Accessed May 2015

McNicholas M (2008) Maritime security: an introduction. Academic, Burlington

Mugridge D (2009) Malaise or farce—the international failure of maritime security. Defense Secur Anal 25(3):305–311

Murphy MN (2009) Small boats, weak states, dirty money: the challenge of piracy. Columbia University Press, New York

Murphy MN and International Institute for Strategic Studies (2007) Contemporary piracy and maritime terrorism: the threat to international security. Routledge for the International Institute for Strategic Studies, Adelphi paper

Nagel T (2005) The problem of global justice. Philos Publ Aff 33(2):113–147

NATO [North Atlantic Treaty Organisation] (2011) Alliance maritime strategy. Available via NATO. http://www.nato.int/nato_static/assets/pdf/pdf_2011_03/20110318_alliance_maritime-strategy_CM_2011_23.pdf. Accessed Apr 2015

Nincic DJ (2005) The challenge of maritime terrorism: threat identification, WMD and regime response. J Strateg Stud 28(4):619–644

Onuoha F (2009) Sea piracy and maritime security in the Horn of Africa: The Somali coast and Gulf of Aden in perspective. Afr Secur Rev 18(3):31–44

Palma-Robles MA (2014) Fisheries crime: bridging the gap. Available via maritime executive. http://www.maritime-executive.com/article/Fisheries-Crime-Bridging-the-Gap-2014-07-30. Accessed Apr 2015

Rahman C (2009) Concepts of maritime security. Victoria University of Wellington No 07/09. Centre for Strategic Studies, New Zealand

RAND (2012) Database of worldwide terrorism incidents (RDWTI). http://www.rand.org/nsrd/projects/terrorism-incidents/about.html. Accessed May 2015

Rawley C (2011) Al Qaeda's seapower strategy. Small Wars J 7

Reveron DS, Mahoney-Norris K (2011) Human security in a borderless world. Westview Press, Philadelphia

Roosvelt FD (1941) Four freedoms speech, annual message to congress on the State of Union: 01/06/1941. Available via Franklin D. Roosvelt Presidential Library and Museum. http://www.fdrlibrary.marist.edu/pdfs/fftext.pdf. Accessed Mar 2015

Sakhuja V (2010) Security threats and challenges to maritime supply chains. UNDIR Disarmament Forum no. 2, pp 3–11

Thai VV (2009) Effective maritime security: conceptual model and empirical evidence. Marit Policy Manag 36(2):147–163

UK [United Kingdom] (2014) The UK national strategy for maritime security, London

UN (2004) A/59/565. UN General Assembly, New York

UNDP (1994) Human development report. United Nations, New York

UNODC (2011) Transnational organised crime in the fishing industry. United Nations Office on Drugs and Crime, Vienna

US [United States] (2015) A cooperative strategy for 21st century seapower

Witbooi E (2015) Towards a new 'fisheries crime' paradigm: challenges and opportunities with reference to South Africa as an illustrative African example. Mar Policy 55:39–46

Wolff S (2006) Ethnic conflict: a global perspective. Oxford University Press, Oxford

World Bank (2010) World development report 2011: conflict, security and development. Available via World Bank. http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2010/03/01/000350881_20100301084958/Rendered/PDF/526500BR0REPLA1cM20101000101PUBLIC1.pdf. Accessed Mar 2015

Pandemic Influenza Planning for the Mental Health Security of Survivors of Mass Deaths

Marie-Jo Medina

Abstract Influenza A pandemics have been documented to occur at 10- to 50-year intervals—an average of three events per century, dating back from the 16th century. Each recorded pandemic has resulted in an increase in annual mortality rates in the infected population, with mass deaths in one pandemic wave equalling fatalities sustained over six months of an epidemic season. This chapter aims to rectify the oversight in pandemic preparedness plans by presenting a compendium of guidelines and recommendations by international health organisations, pandemic fatality experts, and experienced mass death management professionals. Its objective is to have available a mass fatality framework to complement the WHO Pandemic Influenza Preparedness and Response (2009) guideline, from which individual national pandemic preparedness plans are based. It is written in a format that incorporates WHO's emphasis on finding the ethical balance between human rights and successful plan implementation; the assimilation of national pandemic plans with existing national emergency measures; and the 'whole group' system of engaging individuals, families, localities, and business establishments in the process. This chapter is also written such that it can be made applicable to analogous infectious disease outbreaks such as SARS and Ebola, as well as comparable mass fatality events.

Keywords Influenza · Pandemics · Fatalities

M.-J. Medina (✉)
University of Leicester, Leicester, UK
e-mail: mjm50@leicester.ac.uk

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_5

1 Introduction

1.1 Pandemic Influenza

Influenza A pandemics have been documented to occur at 10- to 50-year intervals —an average of three events per century, dating back from the 16th century (Kasowski 2011; Taubenberger 2006; WHO 2005). Each recorded pandemic has resulted in an increase in annual mortality rates in the infected population, with mass deaths in one pandemic wave equalling fatalities sustained over six months of an epidemic season (Hardin 2009).

The three pandemics in the 20th century occurred in 1918, 1957, and 1968. The latter two have been estimated to have resulted in increased deaths totalling up to four million in people in at-risk groups worldwide, while the former resulted in the mass deaths of approximately 40 million in the otherwise healthy groups (Hardin 2009; Kasowski 2011; Taubenberger 2006; WHO 2005). The 1918 pandemic remains the most fatal pandemic in history; a novel influenza subtype of equivalent virulence is anticipated to result in deaths in approximately 2 % of the current global population (Ibid).

There has so far been one pandemic this 21st century, caused by the H1N1 influenza subtype in 2009. Although its attack rate was characterised as mild, it nonetheless resulted in the global deaths of up to 575,400 people who would not have otherwise perished at that time (Dawood 2012). Approximately 80 % of the fatalities were in populations younger than those who generally decease during influenza epidemics, and the burden was most pronounced in the poorer African and Southeast Asian countries (Ibid).

In 1999, WHO published a guidance on pandemic influenza preparedness as a framework for WHO member-nations, in their attempts to develop a plan against the risk of the occurrence of an influenza pandemic, and to introduce the six phases in the declaration of a pandemic (WHO 2005). In 2005, improvements to the guidance were incorporated in keeping with the International Health Regulations (IHR). In 2009, further revisions were made to consolidate developments that have transpired since the enactment of the 2005 framework (WHO 2009). Pertinent to this discourse is the revision accentuating the prevailing of ethical principles when finding a balance between human rights and successful pandemic plan implementation.

Upholding ethical principles include respecting both the dead and the bereaved throughout the course of the event (Morgan 2006, 2009); handling and disposing of bodies in a dignified manner; and respecting cultural and religious conventions (Ibid). Further, it encompasses the acknowledgement of the diversified vulnerabilities and capabilities of individuals and groups, so that nobody experiences marginalisation and disavowal of support (SPHERE 2004). Vulnerabilities may be physical, such as: gender; age; physical or mental impairment; and HIV/AIDS status. They may also be social, including: ethnicity; religious affiliation; political leanings; and residency status (Ibid).

1.2 Mental Health of Survivors of Mass Deaths

Published literature in psychology suggests that disasters can induce mental illnesses among survivors (Bonanno 2010; Gibbs 2003). The most often affiliated mental health illness in disasters is posttraumatic stress disorder (PTSD). However, several individual symptoms, as well as syndromes, have also been associated with the trauma, albeit not given a specific name (Ibid).

Some research promote that the amount of trauma sustained in a disaster is directly proportional to the severity of the psychological illness. Others assert, on the other hand, that ancillary factors may also contribute to mental health risks. These may include the specific context with which the survivor identifies with the disaster; the emotional and physical distance an individual has from the situation; and the quality and accessibility of the support available (Ibid). Further, there are those who argue that PTSD may be overly estimated; while other, less characterised, symptoms are under-estimated (Bonanno 2010). This dubiousness in the literature has been attributed to the difficulty encountered in assessing psychological consequences sustained in disasters, because of the chaotic nature of the event; and because of the methodological impediments to psychoanalysis (Ibid). To provide a more cohesive portrait of ‘typical’ mental health illnesses following a disaster, George Bonanno and colleagues (Bonanno 2010) compiled data from high quality research and summarised their findings in five categories.

The first category relates to the severity of mental illness brought on by disaster. It was determined that, although consequences of trauma from disasters may range from grief and PTSD to depression and suicidal tendencies, more extreme presentations of the disease have only been observed in a small number of cases. In adults, this accounts for only 30 % of all subjects studied. In youths, acute symptoms in the initial aftermath tend to be severe; however, chronic symptoms tend to be more similar in the adults, not exceeding 30 %. The second category pertains to differences in psychological outcomes and resilience. It is suggested that some survivors overcome the traumas within two years post-disaster; while the more resilient only experience transient symptoms and recover fairly quickly. The Third refers to the factors relating to outcomes, already alluded to above, and theorises that there is no single predictor of outcome. This is because individuals have different risk factors for mental health illness, as well as varied mechanisms for coping with trauma. The penultimate category specifies the risk to interpersonal and community relationships. It acknowledges that, although some affiliations are made stronger by shared traumatic experiences, several indicators suggest that most relationships actually do not survive the experience. Incidentally, the status of their post-traumatic interpersonal relationships also influences their coping mechanisms. Finally, in examining the mental health effects to populations located at a distance from the disaster scene, it has been determined that transient grief may be experienced by these individuals; however, psychological disorders may only be recognisable in those with prior experience in disasters, including those who lost loved ones under similar circumstances (Bonanno 2010).

Lastly, literature suggests that the emotional and psychological traumas among survivors of multiple deaths are compounded when the bodies of their loved ones are not processed with care; this is true irrespective of the age, race, or nationality of the deceased (Gibbs 2003; Morgan 2006). Poorly managed deaths therefore, present a perceivable global mental health risk.

However, despite the globally acknowledged increase in deaths due to infection with novel Influenza A subtypes, and all that is recognised about risks to mental health security in mass fatalities, pandemic preparedness plans remain disproportionately focused on preventing the manifestation of a pandemic and on mitigating morbidities and mortalities, rather than equally addressing mass fatality management preparedness plans.

Mass fatality management preparedness planning is paramount in any influenza pandemic preparedness plan if business continuity is to be expediently achieved, and survivor grief and psychological trauma can be mitigated through the honourable and respectful handling of the remains of the dead.

1.3 Aims and Objectives

This chapter aims to rectify the oversight in pandemic preparedness plans by presenting a compendium of guidelines and recommendations by international health organisations; pandemic fatality experts; and experienced mass death management professionals. Its objective is to have available a mass fatality framework to complement the 2009 WHO Pandemic Influenza Preparedness and Response guideline, from which individual national pandemic preparedness plans are based. It is written in a format that incorporates WHO's emphasis on the assimilation of national pandemic plans with existing national emergency measures; the 'whole group' system of engaging individuals, families, localities, and business establishments in the process; and on finding the ethical balance between human rights and successful plan implementation.

Sources for the guidelines include:

1. Hardin and Ahrens (2009) (Hardin hereafter) authored a chapter specific to influenza pandemic mass fatality management. It delineates the facts from the myths and provides a guideline for mass fatality planning.
2. The Integrated Regional Information Networks (2012) (IRIN), whose purposes are to promote the understanding of regional affairs; to advocate competent humanitarian response; and to advance knowledge-based media reporting.
3. The Metro Boston Department of Homeland Security '*Managing Mass Fatalities Seminar Summary Report*' (2011) (Homeland hereafter). This report focused on the lessons learned by multiple sectors, based on their experiences with mass fatality response.
4. Oliver Morgan's '*Management of Dead Bodies after Disasters: A field Manual for First Responders*,' (2009) (Morgan henceforth) whose aims are to advocate

decent and respectful dead body management; and to increase the likelihood of a successful victim identification.

5. The Sphere project: humanitarian charter and minimum standards in humanitarian response (SPHERE hereafter). It developed the 'universal minimum standards' in humanitarian aid, based on the cumulative experiences of disaster teams and agencies.
6. The UK Home Office 'Guidance on dealing with fatalities in emergencies' (Home Office henceforward). This is a joint publication of the UK Home Office and Cabinet Office, from which was based the London 2010 Olympics pandemic plan, the most successful Olympics yet.

This chapter is written such that it can be made applicable to analogous infectious disease outbreaks such as SARS and Ebola, as well as comparable mass fatality events.

2 Mass Fatality Management Planning

Mass fatality is defined as an event where the number of the dead exceeds available local capacities for appropriate management of human remains (Morgan 2006; Ralph 2015). They may ensue from natural or man-made disasters, or infectious disease pandemics. Mass fatality management planning is highly relevant because of the psychological effects improper handling of dead bodies can have on the survivors (Ibid); and because initial stages of fatality management will determine the final outcome in the unequivocal identification of dead bodies, and the subsequent return of their remains to the rightful relatives (Ibid). The survivors' utmost desire, in disasters, is to unequivocally ascertain the circumstances of their missing loved ones (Morgan 2009). However, this desire may run contra-parallel to the disaster teams' priority—mitigating further consequences of the event (Ibid). A balance between practicality and empathy would therefore, need to be established.

Formulating preparedness plans is made difficult by the necessity of predicting scenarios for which the plans can be rationally devised. Undoubtedly, human imagination will fail to predict every possible scenario, and the disaster that eventually unfolds will be one too unbelievable to conceptualise. Nonetheless, it is imperative that certain assumptions are made, if only to provide planners with a point of reference. When developing pandemic plans, Hardin and Ahrens (2009) suggest five assumptions that would be invaluable. They are:

1. The local community would need to be able to support itself, particularly during a pandemic, when similar events are simultaneously occurring elsewhere, and aid will tend to be diffused.
2. Funeral homes will be rapidly overwhelmed.
3. Resourcefulness will be needed in acquiring inventory essential for body management.

4. Funeral and memorial practices may need to be altered to ensure the expeditious processing of bodies.
5. Friends and family from near and far will be desperate for information.

2.1 *Planning Essentials*

2.1.1 Coordination

Chaos is the immediate aftermath of a disaster (Morgan 2009). Therefore, a coordinated plan put into operation as soon as practicable will be invaluable in managing the disaster area. It is likely that local emergency personnel will be first at the scene, and will already have coordinated disaster plans in operation (Ibid). However, it is important to note that stakeholders, leadership structure and operational procedures in pandemic planning may differ from these and other mass fatality plans (Hardin 2009; Morgan 2009). Hence, it is essential that:

(a) A comprehensive list of stakeholders is included in the plan. These may include:

    1. Emergency management teams
    2. Public Health authorities
    3. Medical and veterinary teams
    4. Medical examiners and coroners
    5. Police
    6. Death registry
    7. Funeral directors
    8. Cemetery and crematorium administrators
    9. Legal professionals
    10. Religious officials and community support groups
    11. Schools
    12. Social well-being advisers
    13. Mental health professionals

(b) Establish a structure of leadership, with absolute authority ascribed to the entity presiding over the management of the dead.
A flowchart with names, responsibilities and emergency contact numbers will be beneficial.

(c) Specify each stakeholder's duties and responsibilities. Provide timelines and benchmarks for the successful completion of each task.

(d) Coordinate resources. A system of real-time stock-taking will be beneficial in the sharing and distribution of essential goods and services.
Stipulate how reimbursement for the use of shared resources will be managed, including realistic timelines for monetary disbursement.

(e) Coordinate with regional and national fatality management plans. Their resources and expertise will be of considerable value, particularly in matters relating to funeral homes, mass communication, logistics, and national and international jurisprudence and aid.

(f) Coordinate with international aid organisations. They have the experience, expertise and resources to respond on short notice.

2.1.2 Stockpiling of Resources

Coordinating resources beforehand (in 1(d) above) should prevent stockpiling of necessities with shortened expiration dates that may later go to waste. It is suggested that funeral directors have stock in circulation that is proportionate to a six-month supply for standard operations, the assumed length of the first pandemic wave. It is necessary to note that (Hardin 2009; IRIN 2012; Morgan 2009):

(a) Embalming fluids tend to have a protracted shelf life.

(b) Affordable caskets will be in great demand, particularly in instances when death occurs in more than one family member.

(c) Cremations will require large amounts of fuel.

2.1.3 Information Management

Copious amounts of information are compiled on the dead and missing, regardless of the size of the disaster. Appropriate management of all information will require human and technical expertise, which may be beyond the capabilities of local communities. Regional authorities are more likely to have trained personnel and modernistic technologies, and may therefore, be best placed to take the lead in information management (Homeland 2011; Morgan 2009).

Mass media are indispensable in communicating with a wide audience during a disaster, and both amateur and seasoned journalists will be among the first at the scene. However, the content of the information they provide as well as the manner in which they dispense their knowledge of the scene may induce stress and anxiety among the survivors. Therefore, it is paramount that members of the press be given every possible opportunity to communicate responsibly and to the best of their abilities (Homeland 2011; Morgan 2009: 19).

Effective information management reduces stress and anxiety among survivors, and augments efforts in successfully recovering remains and identifying the dead. Listed below are the matters that need to be considered (Homeland 2011; Morgan 2009):

(a) Coordinating Information

1. Information hubs need a local and regional presence and should be established in the first instance.
2. Determine who would need to be informed, and what the best method of communication would be, to ensure that information reaches as much of the appropriate target groups as possible.
3. Local centres are best for collecting and providing information on the dead and the missing, and for relaying information on the immediate needs of the grieved.
4. Impose upon humanitarian and aid agencies since they will have first-hand knowledge of the state of the scene, and the kind of support the survivors will need.
5. All information needs to be centralised and synchronised for accuracy, and for promoting the successful tracking of the dead and missing.

(b) The information

1. Foremost is the protection of the privacy of those afflicted and their families.
2. Take advantage of already established methods of gathering information (e.g. surveillance networks; automatic alert systems). Ascertain whether expanding the scope of these systems will be beneficial and can be implemented rapidly.
3. Use a template that covers all the essential information, and that could easily be updated. This would include what is being done; what is known; what is yet to be determined; and where further information will be provided when they become available.
4. An informed decision needs to be taken on when it would be appropriate to report the number of dead, missing and displaced. Too soon, and the numbers are likely to be grossly inaccurate; too late, and the media could be disposed towards exaggeration.
5. Information on the system of search and rescue, and body retrieval, identification, interment and disposal must be provided.
6. Photographs and other identifying information should only be released to the media if it has been determined that doing so would enhance the identification process.

(c) The media

1. Designate a representative with whom the media may liaise.
2. Install an office specific for media relations, preferably as close to the scene as possible.
3. Provide journalists with accurate, confirmable, and up-to-date information as close to real time as practicable, to advance factual reporting and mitigate rumour-mongering. This may be facilitated through regular press briefings or short interviews.

4. Social media is a double-edged sword. Knowledge will be available immediately and in real-time; however, the material will tend to be unedited and prone to bias. If not managed appropriately, it may disrupt fatality plans already in progress.

(d) The public

1. Determine the most appropriate method of providing information to different age groups and social, cultural and economic strata, to avoid marginalisation.
2. Circulate concise information on what procedures need to be adhered to, immediately following a disaster.
3. Vigilance in social media trends is essential.

(e) The survivors

1. Impress upon survivors that help is available. Enumerate what support can and cannot be provided, and where they need to go to receive the specific aid they need.
2. Provide an emergency contact number strictly for the relatives of the missing and the dead.
3. Provide specific information on where relatives need to go and what documents they would need to bring, to facilitate the efficient and expeditious management of enquiries.
4. Specify the process for procuring a death certificate, so that they may be able to make legal and funeral arrangements.

(f) The humanitarians

1. Ensure that humanitarian and aid agencies are provided with accurate information, particularly in regard to the risks from dead bodies, and that they themselves are sharing accurate information to those at the scene.
2. Relief agencies such as the International Committee of the Red Cross may be able to help trace missing persons, if given sufficient information.

(g) The dead bodies

1. Standard pro forma containing basic information should be completed for all bodies.
2. In the absence of an electronic system of data-gathering, hand-written forms may be used. However, extreme care would be needed in writing and in the subsequent transfer onto an electronic format.
3. All manner of original forms must be readily available, should data confirmation be necessary.
4. All items of a personal nature, including photographs, may be included in the database.
5. All information must be accompanied by a chain-of-custody.

2.1.4 Death Management

(a) Death surveillance

In the early stages of a pandemic, scientific intelligence gathered through already established surveillance systems would need to be rapidly apprised of the nature of the virus and the manner of death, through the investigation of the index case. It is recommended that the role of investigator be entrusted to the jurisdictional medical examiner or coroner (ME/c) in two capacities (Hardin 2009):

1. Limited jurisdiction over the dead body in cases when:

   (i) Death fits the profile for an emerging disease that needs laboratory confirmation from body fluids and tissues.
   (ii) Death of a poultry worker from influenza-like illness (ILI).
   (iii) Death from ILI of family members or contacts of poultry workers.
   (iv) Death due to recent travel to a country where pandemic flu strain is circulating.
   (v) First death case in a hospital, requiring tissue samples for virus characterisation.

2. Unconditional jurisdiction in cases when:

   (i) There is no listed attending physician.
   (ii) The deceased is unknown and decedents have not been found.
   (iii) Sudden deaths and fatalities uncharacteristic of those due to a flu virus.
   (iv) Death of incarcerated persons.
   (v) It is essential to public health.

(b) Search for the missing

Death from pandemic influenza generally occurs at home or in group care facilities. In the event that an exceedingly virulent pandemic strain also kills its victims with haste, more will be unable to seek hospital admissions prior to death (Hardin 2009). This would result in the saturation of capacities of care facilities and emergency services, and the delayed determination of death. The delay would greatly impact the efficient management of dead bodies (Hardin 2009; Morgan 2009; Ralph 2015; Home Office 2006). The plan to manage this surge, at the scene of death and in the community, should include:

1. At the scene (Home Office 2006)v

   (i) Procedures to locate the missing and presumed dead.
   (ii) Numbering and photographing the dead (or body parts for non-intact bodies).
   (iii) A mechanism for immediate confirmation of death by ME/c.
   Existing laws may need to broaden the stipulations on who has legal powers to pronounce death.

(iv) Record the date, time and place of death, as well as the testifier's name and contact information, and their affiliated organisation's name and address.

2. In the community (Hardin 2009)

   (i) Designate a phone number for the missing persons' hub where inquiries can be made about the well-being of certain individuals.
   This hub must be interfaced with hospital and healthcare centre systems of admissions and discharges, and with ME/cand death registry logs.
   (ii) There must be a system for the regular advertisement of the hub number in several mass media formats.
   (iii) It is essential that the hub's database be unrestrictedly shared with the police and emergency missing persons' divisions.

(c) Recovery and transport of bodies
Dead body management begins when the remains of the deceased are being recovered (Morgan 2009). Recovery commences immediately after searching of the scene has been completed (Ralph 2015). It could last for days or weeks, but may be protracted in more severe disasters (Morgan 2009). Its priority is the rapid location and retrieval of bodies or body parts, and the deceased's personal effects. Speed in recovery aids in identifying the dead; reducing the psychological impact on survivors; and diminishing the distress often associated with the image and odour of death (IRIN 2012; Morgan 2009).
The recovery scene is often chaotic and uncoordinated because there is an abundance of groups and individuals trying to help, including locals; aid agencies; and military and civilian search and rescue operatives (Morgan 2009). In order that body recovery does not impede the simultaneous assistance offered to survivors, the following should be considered (Hardin 2009; Home Office 2006: Morgan 2009):

1. Identify the strictures resulting from the immediate surge in numbers of dead bodies.
2. A balance is needed between speed of recovery and thorough documentation.
3. Appropriate body recovery procedures:

   (i) Use of photographic equipment and standard documentation materials such as body tags with unique references.
   Documenting the exact place and date of recovery would augment the identification process.
   (ii) Impermeable body bags are ideal for recovery, and double-bagging is preferential; however, sheets of any material may be used if nothing else is at hand.
   Each body part must be collected in separate bags and no attempts must be made to match them at the scene.

(iii) Personal items ought not to be separated from the owner, and all documentation must remain with the body.

(iv) Establish two teams: one to take bodies to a holding area prior to delivery; the other to deliver them for either immediate identification or temporary storage for subsequent identification.

(v) The holding area will have rapid turn-over. Hence, it is best situated within close proximity of the scene; preferably stretched across the inner scene cordon.

The holding area is a private and secured space where documents can be cross-checked and evaluated for completeness. At no point must this area be used as a mortuary; a facility for victim identification; or as a temporary storage facility.

(vi) Transport can be achieved by using the body bags or sheets with which they are covered, or by trucks and trailers; however under no circumstances must ambulances be used, as the living are best served by them.

4. Disaster areas may be hazardous. It is paramount that recovery teams not be exposed to undue risks in performing already stress-filled tasks. Risk assessments are requisite and basic health and safety measures must be in place (Home Office 2006; Morgan 2009).

(i) Ventilate enclosed spaces before attempting recovery.

(ii) At the minimum, protective clothing would include disposable biohazard suits; sturdy boots and durable gloves. Face masks may be provided, if only to alleviate anxiety from odours and from fear of aerosol infections.

(iii) Personnel need appropriate training in donning, doffing and decontaminating protective equipment.

(iv) A mechanism of hand-washing, disinfection and decontamination should be available.

(v) First Aid and emergency treatments will be needed on-site.

(vi) The need for vaccination and prophylaxis would have to be evaluated.

(d) Temporary storage and interment

Mass fatalities are expected to overwhelm local surge capacities which will invariably result in delays in victim identification. Further identification delays can result from the logistics of assembling a forensics team, which can take weeks; and from natural decomposition. Places in hot climates are especially vulnerable to decomposition, resulting in bodies becoming unrecognisable within 12–48 h.

To maximise every opportunity of successfully identifying bodies, temporary storage facilities are compulsory. These can be in the form of cold storage or transitory interment (Hardin 2009; IRIN 2012; Morgan 2009; SPHERE 2004). It is imperative that bodies or body parts are stored in the bags or sheets in which they were recovered and that their associated unique identifying tags are written on water-impermeable labels, rather than on the bodies or bags themselves (Ibid).

1. Cold storage

    (i) Refrigeration from 2 to 4 °C will slow decomposition for a maximum of 6 months.

    (ii) Types to consider:

    1. Chilled shipping crates have the capacity to hold approximately 50 bodies.
    2. Air-conditioned trucks can store as many as 30 bodies without the need to build shelving units.
    3. Refrigerated lockers or warehouses may be used.

    (iii) Storage facilities require:

    1. A means of controlling temperature and biohazards.
    2. A mechanism for containing biohazards.
    3. Suitable water supply.
    4. Proper lighting.
    5. Work and rest areas for staff.
    6. A system of communicating with trace and emergency operations.
    7. Shelving units that: are capable of carrying several bodies securely; allow for ergonomic shifting of bodies; and can be efficiently decontaminated at a later time.
    8. Thorough records of every stored body or body part.

    (iv) Shortage of refrigerated storage at the scene is to be expected. Establish a back-up plan until more coolers become available.

    (v) Dry ice may be used in the interim

    1. Overlaying dead bodies with dry ice creates forensic artefacts, and should therefore, be avoided.
       Instead around small groups of bodies, construct a wall of dry ice approximately 0.5 m in height, and secured with durable plastic sheeting.
    2. Ventilate areas where dry ice is in use.

    (vi) The use of ice is impractical and problematic.

    1. A large inventory is required, particularly in instances when rapid melting occurs.
    2. Melted run-offs may pose concerns about diarrheal infections.
    3. Appropriate disposal of ice water will complicate management plans.
    4. Water may distort bodies and destroy personal properties.

2. Interment is the burial of bodies underground when there are no other alternatives, and when temporary storage is needed for longer periods.

   (i) Efficient disinterment will be aided by proper grave construction.

   1. Use a familiar and protected plot of land.
   2. Bury bodies individually if at all possible. Otherwise, use trenches.
   3. Local practices may dictate how bodies are positioned (e.g.: facing Mecca).
   4. Burials should only have one level; be at least 1.5 m in depth; and have parallel spaces 0.4 m in between bodies.
   5. Bottoms of graves with less than 5 occupants should be at least 1.2 m away from ground water. This space should be increased to at least 1.5 m if buried in sand, and at least 2 m if many more bodies are interred.
   6. Tag each body, and record their positions above the grave. Use of GPS systems will be invaluable.

   (ii) Selecting burial sites

   1. Assess soil characteristics, height of water table, and available tracts of land.
   2. Situate in land acceptable to local communities.
   3. Establish in areas easily accessible to mourners.
   4. Sites should be at a distance of at least 10 m from developed land, and 200 m from sources of water, depending on local topographical conditions.

   (iii) Unceremonious burial in mass graves does not satisfy any public health interests; is socially unacceptable; and may waste inventory.

   (iv) Avoid rushed and unmannerly cremations.

   (v) It is disrespectful to gather the dead using backhoes, diggers, or bulldozers.

   (vi) SPHERE international standards mandate that:

   1. Bodies are disposed of with dignity
   2. Cultural and religious practices be honoured
   3. Public Health practices be upheld.

   (vii) Where burial is inconceivable due to frozen tracts of land or lack of solid ground, it may be necessary to store bodies for the duration of a pandemic wave.

   (viii) Survivors are more likely to spread infectious diseases than dead bodies, except in cases where diarrheal diseases and haemorrhagic fevers are indicated.

1. Tuberculosis, Hepatitis B and C, and diarrhoeal diseases can survive for up to 2 days in dead bodies.
2. HIV may survive for up to 6 days.

2.1.5 Identification and Death Certification

Establishing the identity of the deceased is the second major function of incident response teams, following search and recovery, and is generally the responsibility of the ME/c (Ralph 2015). Identification is accomplished by making a match between the information collected about the deceased, and the information documented on the missing and presumed dead (Morgan 2009). The sooner a positive ID is accomplished, the better for the relatives waiting to bury their dead and to go through the legal procedures (Ibid).

Visual identification through decedent recognition or photography is the most basic method of identification (Home Office 2006; Morgan 2009; Ralph 2015). However, mistaken identity is common with this practice, particularly when the dead is soiled or already decomposed (Ibid). Further, viewing multiple dead bodies may have psychological effects on the witness, thereby diminishing the legitimacy of the identification. Errors in identification cause embarrassment to all involved; distress to the relatives; and difficulties with legal issues (Morgan 2009). Therefore, forensic methods would also need to be employed. The success of forensic identification is enhanced by the initiative and diligence of the death management team (Ibid).

(a) Morgue operations

Identification is carried out in the morgue, where the cause and manner of death are also determined. The ME/c determines where the incident morgue is eventually established (Hardin 2009; Home Office 2006; Ralph 2015); it may be that a temporary facility is constructed, or that an already existing structure is expanded to accommodate the surge (Ibid). The benefits and drawbacks of each type of facility would need to be judiciously considered (Ibid).

1. Things to consider:

    (i) Determine how soon temporary mortuaries can be commissioned for use, compared to how quickly expanded space in already built mortuaries can be made available in disasters.

    (ii) Commissioning time will have a direct impact on body recovery, storage, and transport.

    (iii) Temporary facilities need to be operational as soon as 24 h post-disaster.

    (iv) The use of previously functional morgues may mean that storage already contain bodies; hence, surge capacity will be unknown until such time as the disaster occurs.

    (v) The disaster scene will be instrumental in determining the necessity of constructing temporary facilities. Information on the projected number of afflicted; the disposition of the dead; and the estimated time of recovering their remains, all need to be considered.

(vi) In the event that a pandemic is caused by a CBRN attack, the mortuary will be fundamental in criminal investigations; hence, standard operating procedures must be such that substantiation does not fail under legal scrutiny.

2. Mortuaries may comprise of several stations, grouped according to specialities. These may include:

   (i) Admitting area
   (ii) Photography and videography
   (iii) Radiography
   (iv) Personal Effects
   (v) Anthropology
   (vi) Forensics
   (vii) Odontology
   (viii) Fingerprinting
   (ix) Pathology
   (x) Repository
   (xi) Transport
   (xii) Embalming

3. Categories for a positive identification

   (i) Primary—only one of these is necessary

      1. Fingerprints.
      2. Dental.
      3. DNA.
      4. Unique identifiers such as serial numbered artificial limbs and implants.

   (ii) Secondary—two or three are needed

      1. Personal accessories such as jewelry, driver's licence, or identity card.
      2. Bespoke apparel.
      3. Tattoos, scars, birthmarks or physical deformities.
      4. X-ray detailing limb fracture history or active tumours.
      5. Blood and tissue type.

   (iii) Visual—Prudence is vital

      1. Photography.
      2. Basic description of physical features, such as race; height; and eye and hair colour.
      3. Location when found.
      4. Clothing when discovered.

4. Autopsies are not needed to confirm death caused by influenza. However, if they are performed, some guidelines apply:

    (i) In the interests of public health, respiratory tract and tissue samples for laboratory analyses may be collected.
    (ii) Liaising with public health laboratories on the current guidelines for collecting and transporting influenza specimens will save time and effort.
    (iii) Next-of-kin will generally need to give permission for the autopsy to be performed in a hospital.
    (iv) ME/cs do not need permission if the autopsy is within their remit.

5. Release of bodies to relatives

    (i) Release dead bodies only when a definitive identification has been made.
    (ii) Expedited release may be necessary where cultural or religious customs are indicated.
    (iii) Some laws stipulate who has the authority to perform this task.
    (iv) The name and contact details of the claimants need to be collected and filed along with other documents associated with the body.
    (v) Unidentified bodies, foreign nationals, undocumented migrants, and homeless persons need to be stored or interred for further identification at a later time.
    (vi) Release of bodies with missing parts may later impede the management of severed body parts. To minimise complications, family members' wishes regarding future identification of other body parts should be documented. Choices may include:

        1. To postpone body release until all body parts have been found.
        2. To proceed with the funeral but be apprised of other parts that are later found.
        3. To proceed with the funeral and consider the matter closed.

    (vi) A death certificate is provided with the release of the body.

6. Death certificates

    (i) The death certificate is a legal document; hence, the law stipulates the signatory on the certificate.
    (ii) The document specifies the cause and manner of death; where death occurred; when it was pronounced; and the name and contact details of the signatory.
    (iii) In pandemics, it is essential that hospitals and care facilities assign this task to specific individuals in order to mitigate chaos.
    (iv) Funeral directors with policies against collecting bodies unaccompanied by a certificate of death need to allow for flexibility during pandemics.

1. This should be addressed in the planning stages.
2. All stakeholders must be in agreement.

(b) Funeral homes and crematory operations

Funeral directors are responsible for the recovery and transport of dead bodies; preservation of the integrity of the chain-of-custody; and assistance in disposal of the remains. Although they are not qualified grief counsellors, they are nonetheless tasked with conversing with individuals on the most discomfiting day of their lives. This therefore, also makes them the best people to facilitate the return of the dead to their bereaved relatives (Homeland 2011).

Once a body has been released to the decedents, it is generally their responsibility to contact the funeral director of their choosing, for the transport of bodies to funeral homes and the subsequent burial or cremation, according to their culture or religious beliefs (Hardin 2009; Homeland 2011; IRIN 2012; Morgan 2009; SPHERE 2004).

Pandemics could result in funeral homes overseeing 6 months' worth of dead bodies within a 6–8 week period (Hardin 2009; Homeland 2011; IRIN 2012; Morgan 2009). Therefore, it may be prudent for individual funeral homes to plan for employing more trained personnel who can be available on short notice (Ibid).

1. Transport of dead bodies

   (i) Funeral directors will be responding to requests from families to transport bodies to funeral homes, and from ME/cs to provide conveyance to mortuaries or storage facilities. Plans for the inclusion of more licensed funeral directors and transport services is therefore essential.

   (ii) Safeguard lawful body transport by ensuring that funeral home personnel are licensed and trained in recovery and transport, and that their vehicles are approved and registered for carrying dead bodies.

2. Burial or Cremation

   (i) Burials are more practicable in disasters, because they enable future identification of persons yet unknown.

   (ii) It is not good practice to cremate the remains of unidentified bodies.

      1. There is no public health benefit in cremating those who die of influenza.
      2. Cremation will not allow identification in future.

   (iii) Cremating one body takes 4 h and produces 3 to 6 pounds of ash and partially incinerated body parts; thereby, creating logistical difficulties when the number of bodies rapidly mount.

(a) The feasibility of continuous running of furnaces need to be determined, particularly in residential areas.
(b) If licensing laws are in place, they may need to be lifted.

3. Embalming

   (i) To be performed only when requested by families who would rather not have their dead cremated.
   (ii) Expediting the process may be necessary.

4. Death registration

   (i) Funeral directors are normally responsible for registering deaths, after receipt of a death certificate.
   (ii) Funeral directors collect demographic information from family members, prior to registration with a vital statistics office.
   (iii) Electronic submission of both death certificate and registration would be well-placed during a pandemic.

(c) Waste disposal

1. Flush liquid waste per standard practice, without the need for pre-treatment.
2. Consult the jurisdictional wastewater treatment facility before dumping large volumes of liquid waste down the drain.
3. Dispose of solid waste in biohazard containers for subsequent incineration.

2.1.6 Family Support and Assistance

Family Assistance is one of the most sensitive undertaking in mass fatality management. Family Assistance Centers (FAC) are generally established near mass fatality scenes, where survivors can congregate to wait to hear about the status of their missing, and to receive much-needed support (Homeland 2011; Morgan 2009; Ralph 2015). FACs are secure, private, and multi-sectorial, so that all the support and assistance needed can be provided under one facility (Ibid). Things to be considered in establishing FACs include:

1. Function of FAC

   (i) To provide families with information on their missing and dead.
   (ii) To provide shelter from media intrusion and from the newsmongers.
   (iii) To enable investigators and ME/cs to gather information from families about the missing and the deceased.

2. Facilities

   (i) Situate FACs near the disaster scene, where ingress and egress can easily flow.
   (ii) Avoid locating FACs near the morgue.

(iii) Ensure the area is secure and private.
(iv) It needs to be accessible for 24 h within the first 3 days, after which it can be scaled down to operate for 14–16 h a day.
(v) Anticipate approximately 10 kinsperson for every victim and plan accordingly.
(vi) Multiple FACs may be necessary, but movement of families from one area to another must be avoided; instead, FAC personnel should go to where the survivors are situated.
(vii) Facilities must be scalable.

3. Support and assistance

(i) Prioritising the needs of the vulnerable.
(ii) Personal and private meetings with family members as soon as practicable to initiate the collection of ante mortem information for the mortuary.
(iii) System for reporting and providing information on the missing.
(iv) Emotional and psycho-social support for survivors befitting their needs, culture, and the context of the disaster.
(v) Systematic, up-to-the-minute information on the missing and the dead. Families ought to be the first informed of the status of their loved ones.
(vi) Realistic timeframes for searching for the missing, and recovering and identifying of the dead.
(vii) Opportunities for survivors to view their dead.
(viii) Presence of religious leaders who could help survivors understand and reconcile their beliefs with the processes of body recovery and identification.
(ix) Prioritise the needs of vulnerable groups.
(x) Reunification of displaced minors with their family as much as practicable.
(xi) Material and financial support for funerals.
(xii) Legal assistance
(xiii) Translators for foreign language speakers.

4. Agencies and Staffing

(i) Each support agency within FACs needs a command post; a separate area for staff preparation and duty operation; and the capability to deploy staff to FAC.
(ii) The nature of the disaster will determine which agencies are involved. Frequently in force are family assistance services; mental health assistance; and child agencies.
(iii) Aid agencies and faith groups may be present.
(iv) FAC staff must be vetted.
(v) Flexibility is essential in order to accommodate the changing needs of the families as time progresses.

3 Conclusions

Based on the history of influenza A pandemics, this century may be due for, at most, two more pandemics. If even one of them is as deadly as that of 1918, then approximately 2 % of the global population will die. However, even if the future 21st century pandemics are atypically mild as that of 2009, still many more people will die than normally would.

The WHO provided a framework for influenza pandemic preparedness planning. However, its focus is skewed towards the prevention of the event from happening, and a bit remiss on planning for the management of the surge in deaths. Having a fatality management plan incorporated in pandemic plans is relevant because mishandling of dead bodies is a mental health risk for their loved ones.

Mass fatalities may ensue from natural or man-made disasters, or infectious disease pandemics. Regardless of how they may transpire, conflict will invariably come to pass between the fatality management team, and the surviving relatives of the missing and the dead. Conflict is inevitable, because each group contextualises the event from different perspectives; fatality management personnel perceive the event as something that needs immediate oversight, in order that they may mitigate further calamitous consequences; survivors, on the other hand, are more single-minded in their overwhelming desire to determine the circumstances of their missing loved ones (Morgan 2009). However fatality management ultimately eventuates, respect; sympathy; and caring are due the dead and their relatives throughout the event (Ibid).

References

Bonanno GA, Brewin CR, Kaniasty K, La Greca AM (2010) Weighing the costs of disaster: consequences, risk, and resilience in individuals, families, and communities. Psychological Science in the Public Interest 11(1):1–49

Dawood FS, Juliano AD, Meltzer MI, Shay DK, Cheng P, Bandaranayake D, Breiman RF et al (2012) Estimated global mortality associated with the first 12 months of 2009 pandemic influenza A H1N1 virus circulation: a modelling study. Lancet Infectious Diseases 12:687–695

Gibbs M, Montagnino K (2003) Disasters, a psychological perspective. Available online at: http://training.fema.gov/hiedu/docs/emt/gibbspsychology.doc. Accessed 9 May 2015

Hardin LJ, Ahrens JP (2009) Fatality management during a pandemic. In: Ryan J (ed) Pandemic influenza emergency planning and community preparedness. CRC Press, Boca Raton, pp 207–236

Homeland Security (2011) *Managing mass fatalities seminar: A summary report*, Boston: Metro Boston Homeland Security. Available online at: http://delvalle/assets/pdf/Managing%20%Mass%Fatalities_Report%2004-13-2011.pdf. Accessed August 01, 2014

Home Office and Cabinet Office (2006). *Guidance on dealing with fatalities in emergencies*. Available online at: http://www.gov.uk/government/publications/guidance-on-dealing-with-fatalities-in-emergencies. Accessed May 8, 2015

Kasowski E, Garten R, Bridges C (2011) Influenza pandemic epidemiologic and virologic diversity: Reminding ourselves of the possibilities. CID 52(Suppl. 1):S44–S49

Morgan O, Sribanditmongkol P, Perera Sulasmi Y, van Alphen D, Sondorp E (2006) Mass fatality management following the South Asian Tsunami Disaster: Case studies in Thailand, Indonesia, and Sri Lanka. PLoS Medicine 3(6):e195

Morgan O, Tidball-Binz M, van Alphen D (2009) (eds.) (3rd ed) Management of dead bodies after disasters: a field manual for first responders. PAHO, Geneva

Ralph, T. (2015). '*Mass Fatality Management*', *Disaster resource Guide*. Available online at: http://www.disaster-resource.com/index.php?option=com_content&view=article&id=347:mass-fatality-management&catid=9:crisis-response&Itemid=15. Accessed April 20, 2015

The Sphere Project (2004) The Sphere Project. Oxfam Publishing, Geneva

The Integrated Regional Information Networks (2012). '*Analysis: Why dead body management matters*', *IRIN humanitarian news and analysis*. Available online at: http://www.irinnews.org/report/96673/analysis-why-dead-body-management-matters. Accessed May 8, 2015

Taunbenberger J, Morens D (2006) 1918 influenza: The mother of all pandemics. Emerging Infectious Diseases 12(1):15–22

World Health Organization (2005). *WHO global influenza preparedness plan: The role of WHO and recommendations for national measures before and during pandemics*. Available online at: http://www.who.int/csr/resources/publications/infelunza/WHO_CDS_CSR_GIP_2005_5.pdf. Accessed January 02, 2014

World Health Organization (2009). *Pandemic influenza preparedness and response: A WHO guidance document*. Available online World Health Organization (2011). *Avian influenza*. Available online at http://www.who.int/Mediacentre/factsheets/avian_influenza/en/index.html. Accessed December 4, 2012

An Evaluation of the Police Response to Gang-Related Violence and Future Security Threats

Paul Canfield

Abstract Over the past decade Bermuda has experienced a dramatic increase in gang violence. The United Nations Office on Drugs and Crime's Global Study on Murder showed that Bermuda's murder rate had increased from 3.1 per 100,000 people in 2003 to 12.5 in 2011 (Strangeways in *The Royal Gazette*, 2010). While the increased prevalence of gangs is not something that is unique to Bermuda (Bullock and Tilley in *Shootings, gangs and violent incidents in Manchester: developing a crime reduction strategy*. Home Office, London, 2002; Battin-Pearson et al. in *Gang membership, delinquent peers, and delinquent behavior. Youth Gang Series*. Washington, 1998), the sharp increase was a cause of great concern within the local community, the police and politicians (Parliamentary Joint Select Committee in a parliamentary joint select committee publication under part IV of the Parliamentary Act 1957, 2011). The reason for this may be that Bermuda's economy relies largely on tourism (Central Intelligence Agency in The World Factbook. The Central Intelligence Agency, 2013) and international business, especially reinsurance, which increased its presence on the island since the terrorist attacks in New York and Washington on the 11th of September 2001. Any increase of gang violence in an otherwise peaceful and low crime country may deter future investment in the island (Washington Post in *Gang violence jolts formerly quiet Bermuda; tourist getaway grapples with string of shootings*, 2006). This research primarily seeks to outline the development of Bermuda's gang culture and how the Bermuda Police Service (BPS) responded to the gang violence. It has been suggested that gang-related crime is essentially a social problem and not just an undertaking for the police, but the community as a whole (Muncie in Crime Justice Matters 34:4–5, 1999). Socio-economic factors may have also influenced the development of gang crime in Bermuda, but this research focuses on the situational

P. Canfield (✉)
University of Leicester, Leicester, UK
e-mail: canfieldp@me.com

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_6

crime prevention strategies that the BPS adopted and whether these strategies have helped to reduce gang violence, and whether the techniques used may be considered suitable in preventing a rise in terrorism.

Keywords Gang-related violence · Terrorism · Policing · Bermuda

1 Introduction

New security threats such as international terrorism, organized crime, natural disasters, pandemics, drug trafficking are shaping security agendas globally. Over the past decade Bermuda has experienced a dramatic increase in gang violence. The United Nations Office on Drugs and Crime's Global Study on Murder showed that Bermuda's murder rate had increased from 3.1 per 100,000 people in 2003 to 12.5 in 2011 (Strangeways 2010). Although the increased prevalence of gangs is not something that is unique to Bermuda (Bullock and Tilley 2002; Battin-Pearson et al. 1998), the sharp increase was a cause of great concern within the local community, the police and politicians (Parliamentary Joint Select Committee 2011). The reason for this may be that Bermuda's economy relies largely on tourism (Central Intelligence Agency 2013) and international business, especially reinsurance, which increased its presence on the island after the terrorist attacks in New York and Washington on the 11th of September 2001. Therefore, any increase of gang violence in an otherwise peaceful and low crime country may cause heightened feelings of fear and terror amongst the population, and as such may deter future investment in the Island (Washington Post 2006).

In the same decade, in the aftermath of the deadly attacks on the Twin Towers by Al Qaeda, many predicted that such was the current threat of terrorism, an increase in the 'militarisation' (using primary-situational crime prevention methods), of western cities and nations would occur (Briggs 2005). Many different tactics have been employed by terrorists in recent times, including indiscriminate attacks involving assassinations, hijackings, bombings, shootings, arson and sabotage listed among many of the approaches used (Drake 1998). Several attacks have taken the form of many of these categories and have largely focussed on indiscriminate mass-killings of individuals using a combination of guns, explosives and bladed articles to target businesses and public spaces, causing terror, chaos and damage to the economy . This more recent fourth-wave of religiously-motivated attacks have been repeated in several cities including Mumbai 2008 (Friedman 2009; Schifrin 2009), London 2005, Paris 2015, Sydney 2015, Madrid 2004, and across several continents including North America, Africa and the Middle East. Arguably many other attacks fail (Bakker 2006), but *all* are generally seen as a one-way trip for the attackers, and while most are not described as suicide attacks, many of the assailants would not have expected to live or avoid capture once the security response was activated (Drake 1998). This tactic of large-scale indiscriminate killing has been closely attributed to religious terrorism (Pedahzur 2004) and many of these attacks have furthermore been described as an evolved form of '*urban-siege*' (Sullivan and Elkus 2009).

In 2007, the BPS responded to less than ten firearms offences. Between 2008 and 2012, Bermuda witnessed an increase in gang violence involving the use of firearms, resulting in 65 injuries and 24 fatalities (Johnston-Barnes 2011). Since 2003, a total of 30 men have been killed in gang-related violence. While elsewhere in the world not all firearms incidents are gang-related, there is a statistical trend in Bermuda that suggests that the majority of firearms offences committed in Bermuda, certainly all the murders and injuries caused by a firearm during this time have been directly gang-related, even when the victims themselves may not have had a gang affiliation (Johnston-Barnes 2011).

On the face of it, Bermuda's gang violence may appear to be similar to that of other jurisdictions, specifically those involving a turf war over control of the drug market. However, social, geographical and economic factors make Bermuda's gang problem uniquely different (Comeau 2012). While social crime prevention strategies may be more effective in changing social attitudes, reducing gang membership and associated crime in the long-term (Crabbe 2000; Caruso 2011), they do not have the same instant results that situational crime prevention can provide (Ehlers and Tait 2009: 25), and it may be possible to measure the impact of these prevention techniques between 2003 and 2014.

However, the greatest concern for Bermuda should not only be restricted to the evidence of home-grown gang-related violence, but also the current rise of international gang crime and the socio-economic opportunity for the growth of terrorism.

Bermuda has experienced terrorism during the 1970s, when on the 9th September 1972 the Black Panthers assassinated the British Police Commissioner George Duckett. Approximately six months later the British Governor John Sharples and his Aide De-Camp were also murdered. Two weeks afterwards two Portuguese shop owners were also killed. The motives for these murders were '*Black power, anti-colonialism and terrorism*' (Swan 2009). Although this terrorist act occurred 40 years ago, when we consider the revised Academic Definition of Terrorism by Alex Schmid (2012) that include twelve points of note that help to define terrorism, we can assume that future terrorist acts within Bermuda, whilst they appear unlikely, are not improbable.

There are several current threats to Bermuda that could lead to a reoccurrence of such a rise in violent crime or political violence; internationally, there has been a notable increase in gang-related violence in several Caribbean countries (Seepersad and Bissessar 2013); political, social and economic (BBC 2009) disruption and conflict occur frequently across the globe, the effects of which have been seen during the Arab Spring; similar concerns, albeit of a different political background, simmer in Bermuda as protests occur over human rights, immigration concerns, historic land transactions, and work and pay conditions for government workers. In 2010, global droughts and severe storms caused an increase in global food commodity prices, and the US National Intelligence Council estimate that demand for food will increase a further 25 % by 2030 (Rothkopf and Casey 2014) presenting a concern for any small nation that relies solely on the importation of goods. The predicted rise of sea levels over the next century presents a further security risk that could lead to a rivalry for land as coastlines are threatened, but may also act as a driver for mass migration. Despite Bermuda's volcanic topography, even the optimistic prediction of a 1.5-foot rise over the next century (Rothkopf and Casey 2014) should be seen as a significant threat to the political and economic stability of the country; finally the competition for dwindling resources and territory may threaten Bermuda's resource rich Exclusive Economic Zone. A risk that appears to have been overlooked in the Government of Bermuda report (2013) but is currently destabilising the South China Sea region (Faith 2014; Holmes 2015).

Criminal and terrorist organisations may thrive in such unstable environments and rises of association with such groups by disaffected individuals can be seen across Africa, the Middle East, Asia and South America. These groups and ideologies cannot be fully explored in this paper, but it is known that they seek to attack Western interests both at home and abroad using 'Black-swan style' attacks, and regularly change their modus operandi to focus on softer-targets.

When considering that Bermuda seeks to raise it's international profile as a leading destination for international tourism, hosting the America's Cup in 2017, and international business, then it is logical to assume it will present a potential opportunity for terrorist organisations or 'lone-actors'. It has already seen terrorist inspired graffiti referring to ISIS upon several key buildings that may be an early warning to potential future risks (Jones 2015).

> *threat multipliers that will aggravate stressors abroad such as poverty, environmental degradation, political instability, and social tensions – conditions that can enable terrorist activity and other forms of violence.* (Department of Defense 2014).

Therefore, this study primarily aims to establish what may have caused the rise in gang-related violence and if there is any correlation between the use of primary crime prevention techniques by the BPS and crime figures (Nichols and Crow 2004).

Furthermore, this research will discuss the possible effects that the different crime prevention strategies employed by the BPS may have had when tackling modern gang violence, and whether these were effective in Bermuda. It is anticipated that this study will be able to demonstrate that the BPS successfully reduced the immediate problem of gang-related violence.

Any findings may then be used to implement further discussion, research or prevention strategies in the fight against terrorism, gangs and violent crime in Bermuda and in other jurisdictions as this research will suggest that many *similar* prevention techniques may affect the recruitment or radicalisation of individuals into gangs and terrorist organisations. Only by the '*scaling-up of some key resource areas*' to ensure more permanent '*peacebuilding*', and increased policy coordination between state, non-state actors and international partners is the only way to ensure a reduction in membership or growth of such lawless groups (Seepersad and Bissessar 2013).

2 Security Threat—Gang Violence and Organized Crime

There is very little known about the sociology of gangs and there is still debate surrounding an appropriate definition for them (Covey et al. 1997). This in many ways is similar to lack of understanding of the characteristics of global Jihadi terrorist networks (Bakker 2006). However, this research will discuss gangs in Bermuda, applying the theoretical definition as proposed by Klein and Maxson (1989), namely that a group must be involved in *illegal activity* and *maintain a territory*.

An understanding of Bermuda's topographic, geographic and social factors will help to explain the problems that are faced when tackling gangs locally. As Bermuda is small it creates a geographical problem. If gang members wish to cease being a member of a gang they have to leave Bermuda, otherwise they may still be considered a target. Also, family ties are widespread throughout the island and it is not uncommon for families to become targets due to their familial association rather than having a direct gang involvement (Dale 2009; Comeau 2012). Furthermore, disinhibiting factors that may increase the likelihood of violence re-occurring, not only includes the availability of weapons *but* also proximity of offenders to victims (Kemshall 2001; Limandri and Sheridan 1995 cited in Kemshall 2002: 20).

2.1 History of Gangs in Bermuda

The term 'gang' was first used in Bermuda in the early 1900s (Musson 1979), although there is very little evidence documenting their behaviour. Between the 1950s and 1980s gang association was largely related to the differences between Town, those in the central parishes immediately surrounding the City of Hamilton (the capital city of Bermuda), and Country, i.e. locations in the eastern or western parishes. This 'gang' activity stemmed from geographical sporting rivalry (Jones and Whittaker 2009). However, 'political-criminal' gangs and terrorism were also evident during disturbances and killings throughout the 1970s (Swan 2009).

Modern criminal gangs in Bermuda can trace their origins to the early to mid-nineties. A gang called Frontline began to import and sell crack cocaine in Bermuda and built several US east coast ties with gangs in Newark and Philadelphia. Frontline was the most noticeable gang at the time due to the high-profile 'lifestyle' that was associated with them. This was a media-sensationalised-gang-lifestyle based on the American stereotypes (Covey 2003; Decker and Weerman 2005), and created 'push-and-pull factors' surrounding gang membership that typically affect young people (Decker and Van Winkle 1996; Comeau 2012). Soon, 'gangs' began forming in various locations and often became known by their geographic location (Pearman 2011), however not all of them operated as organized criminal entities (BPS 2010a; Pearman 2011).

Initially, during the 1990s, the Bermuda Police Service did not refer to these groups as gangs and preferred to describe them as loosely organized groups (LOGs). This may have been due to the fact that these groups were based around casual friendships and therefore did not meet the definition of a gang (Brymer 1967; Sanders 1994). By the early to mid-2000s, some of the groups had increased their presence, becoming involved in an elevated level of criminal activity and street socialization. This is a common feature seen in the development of gangs (Vigil 2002). As anti-social behaviour, petty-crime and drug use increased at these locations, or 'hot-spots' as they became known (BPS 2002: 24), so too did the police presence.

As these groups became more organized the use of gang names, tattoos, graffiti, signs, jewellery and colours became more prevalent. Conflict between the gangs began to increase and incidents of violence became commonplace. The weapons of choice then, were baseball bats, machetes, knives and to a lesser extent, firearms (BPS 2003: 73). Conflict and violence when defining gangs and gang members, whether with one another, other gangs or the authorities, appears to be an important element of gang behaviour (Hagedorn and Macon 1988; Klein 1995; Sanchez-Jankowski 1991). These interstitial LOGs had morphed into gangs (Thrasher 1927).

Several 'social factors' are thought to have had a catalytic effect on the gang problem in Bermuda (Wilson 2013d). Bermuda's close-knit society has historically made jury selection hard to secure; potential jury members will often know the accused, their family or friends. Further, a lack of anonymity limits the willingness of witnesses to give evidence (Comeau 2012). This is illustrated by the case of Tekle Mallory in which over 100 people witnessed his 2001 murder during a brawl, but the two suspects charged were acquitted on lack of evidence (Bernews 2010c). Consequently Shaundee Jones, one of the few witnesses that did give evidence in the murder of Tekle Mallory was shot and killed in 2003. Again, the suspect charged with the murder was acquitted for lack of evidence. This 2003 incident arguably became the catalyst for the escalation of gang-related violence, and is understood to be the first modern-day gang killing involving a firearm (Strangeways 2011a).

Further incidents occured, in 2006 Jason Lightbourne was shot and killed in what was suspected to be a drive-by shooting in the Ord Road, Warwick area by the Parkside Gang. This could have been the result of increased rivalry between Parkside (a central-parish gang) and the Ord Road Crew. The floodgates then opened in 2009 with many high-profile gang-related murders. Kiwande Robinson, an alleged member of 42, was shot and killed in the St Monica's Road area on May 22nd by members of Parkside, with another male being injured (Strangeways 2011b). Kumi Harford, who was considered a high-ranking member of the 42 Gang (a western-parish gang), was shot and killed on the 5th December 2009 by Antonio Myers, a high-ranking member of the Middletown Gang (associated with Parkside). Myers was convicted of this crime in 2011 and sentenced to 38 years in prison (Bernews 2010a, b, c, d, 2011a). Similarly, an unknown suspect murdered Gary Cann, believed to be a Parkside affiliate, on the 15th December 2009 in rival territory.

Parkside, based in the City of Hamilton, and the 42 Gang, based in North Pembroke, initially shared some of their senior membership. While it is not fully known what caused the split, it is suspected that it was over control of the drugs market. The rivalry between the two gangs lasted for over ten years, resulting in a deadly history of violence that quickly included murder and attempted murder (Strangeways 2011c).

During 2009, a significant increase in retaliatory gang murders and shootings was experienced which continued for the next few years. As a result Bermuda had a per capita murder rate higher than New York and more than five-times higher than London.

The murder rate in Bermuda further increased in 2011 giving it a murder rate of 12.3 per 100,000 people. This put Bermuda between Nigeria (12.2) and Swaziland (12.9) on the world list of dangerous countries (BBC 2006, 2010).

2.2 Current Overview of Gangs in Bermuda

During 2013, three more gang-related murders were recorded. However, on the whole, crime and gang-related violence decreased significantly since 2009 (Pearman 2011). Bermuda is currently experiencing, what many hope is more than just a lull in gang violence (Bell 2014), with only two gang-related murders in 2014, and one so far in 2015. However, during 2015 there has been an increase of armed robberies, stabbing murders and several people have been injured by gunfire.

The gang-scene has however, changed dramatically since 2009. The 42 Gang no longer exists; many of their members have been murdered or are incarcerated with lengthy prison sentences. Currently, Parkside and MOB are the dominant gangs in the central and western parishes respectively, although overall there has been a decline of overt gang activity; a diminished street presence, fewer gang tattoos, less overt gang jewellery and gang members have started to conceal their gang affiliation (Pearman 2011).

3 Understanding Crime and Gangs: Theories and Concepts

3.1 Crime Rate as Pertains to Gangs

The development pathway to serious and violent behaviour was developed by Loeber et al. (1998: 247) and demonstrates that gangs and delinquency are closely linked. Furthermore, gang involvement increases the exposure to risk factors and this in turn increases the possibility of persistent serious offending by the individual (Stouthamer-Loeber et al. 2002).

There is evidence suggesting that an increase in gangs resulted in an increase of violent crime in the US during the 1980s (Curry and Decker 2003: 28). Several studies conclude that one third of murders in Chicago (Block and Block 1993); around half of the murders in one Los Angeles district (Tita et al. 2003), and an even higher amount of youth murders in Boston are gang-related (Kennedy et al. 1996). Furthermore, studies of gang crime in the United Kingdom record around 60 % of shootings being gang-related (Bullock and Tilley 2002). Bermuda has a higher percentage of shootings and murders attributed to gang-related activity than any of these (BPS Quarterly Statistics).

Several youth studies indicate that juvenile gang members commit much higher acts of delinquent crime than their peers. They can commit up to five times the amount of offences against the person and as high as twelve times the amount of drug offences (Esbensen et al. 2001; Thornberry et al. 2004). However, there appears to be a significant disparity between youth surveys that demonstrate a high percentage of crimes being attributed to gang members, and overall crime figures, which have a comparatively low percentage (Curry and Decker 1996). Although gang membership increased in the US after the 1980s, this was not reflected in a decline of criminal violence throughout the 1990s (Blumstein and Wallman 2000) and although gang-related murders within some US cities have been extremely high (Decker and Curry 2003), they account for only up to 16 % of the total murder rate for the US (Klein and Maxson 2006).

Gangs are by and large composed of delinquent youth who appear statistically inclined to carry out more violent crime than their peers. It would therefore follow that gangs are responsible for a significant share of crime (Kennedy 2011). This is examined together with the understanding that a minority of chronic offenders (Farrington 1992: 534) who number between 4 and 8 % of the population (Wyrick 2006) are responsible for the majority of crime that occurs, even in less affluent neighbourhoods. In addition, it is known that 7 % of the US prison population is responsible for more than half of all the violent crime reported, with recidivism rates as high as 76 % (Jennings 2006: 38). In light of these facts, the premise that gang members commit more crime is supported, especially in some inner cities where gangs are understood to be responsible for around 80 % of the crime (Ryan 2009).

However, care needs to be exercised when relying on crime data such as arrest figures, conviction and recidivism rates to ascertain if gangs commit more crime. Police arrests do not automatically ensure a conviction. Similarly data based on convictions may well underestimate the actual involvement in crime by an individual (Friendship and Thornton 2001). Furthermore, the United Nations (2011) has stated that in certain regions firearms undoubtedly act as the driver of murder rates and these are usually in the hands of organised criminal groups.

3.2 *Situational Crime Prevention Theories*

Situational crime prevention aims to reduce the opportunity for offending by making crime harder to commit, by shifting the balance of consequence outweighing the reward. Also known as ‘Crime Prevention through Environmental Design’ (CPTED), it may be achieved by target hardening, defensible space architecture (Newman 1972), community crime prevention initiatives and ‘top-down’ initiatives.

The *fear of crime* may be as prevalent as crime itself and situational techniques appear suitable for addressing the fear of crime while also preventing it occurrence (LaCourse 1994).

There is empirical validity in successful situational crime prevention methods being implemented (Clarke 1997). Poyner and Webb (1987) were able to demonstrate that an increase in situational techniques on a British housing estate (cameras, electronic access to properties and fencing) caused a significant reduction in damage and theft offences. Similarly, Bullock et al. (2010) were able to show that the police escorting of British football fans to and from stadiums reduced disorder and affray by limiting confrontation and provocation between rival groups. Several criticisms of situational prevention techniques exist, although many of these may also have positive effects. ‘Displacement’ may occur where crime moves to a more unmonitored location and continues (Smith and Clarke 2012). It must be recognized that sometimes crime displacement may be the desired result (Weisburd et al. 2006);

‘Escalation’ may occur, when situational prevention techniques lead to the commission of more serious crimes (Grabosky 1996). For example, aggressive police interdiction or longer prison sentences may result in a defiant reaction rather than act as a deterrent. Harsh carceral measures may however, legitimately reduce the fear of crime (LaCourse 1994). However, the US has one of the largest prison communities in the world and still has fears over an increasing crime rate (Skinner 2013; US Congress 2013; US Sentencing Commission 2011). Ironically, rather than having the desired effects on the prison community, incarceration may actually encourage increased criminality (Foucault 1980).

‘Creative adaptation’ is where crime finds a way to continue despite the applied situational techniques (Weisburd et al. 2006). This may be as simple as a drug dealer not carrying drugs upon his person (BPS 2003), to victims being kidnapped and forced to allow access to money (Pharoah 2005). Situational crime prevention has also been criticized for an ‘absence of permanency’. Initial preventative actions need to be sustainable (Weisburd et al. 2006), and financial support may not always be achievable (Loveday 1994 cited in Kelly et al. 2005).

Increased police patrols leads neatly to ‘over-deterrence’ or having an impact on the civil rights of society. Certain implemented techniques may have negative effects on legitimate activity and daily routines (Parnaby 2006; Coleman 2003a, b). Finally, and most importantly, some situational crime prevention techniques are not effective in reducing violent crimes or crimes of passion (Geason and Wilson 1988). This factor is increasingly important when considering the acts of gang-related violence and terrorism that occur.

However, there are many documented examples of successful situational crime prevention methods (Clarke 1997). Situational prevention appears to be easy to measure and monitor through increased reporting techniques and the monitoring of calls to the police.

One of the biggest problems when attempting to respond to ‘crime’ is being able to understand the problem correctly (Her Majesty’s Inspectorate of Constabulary 2012: 3; Decker 2003). Research suggests that law enforcement agencies tend to conduct only a superficial analysis of the problem and in some circumstances, in what is seen as a knee-jerk reaction, rush to implement responses that tend to mask the problem rather than address the cause (Cordner 1998). However, these agencies are required to respond in a reactive manner as well as being proactive to ensure that problems are effectively nipped in the bud from both sides. The problem with implementing and relying on traditional or faddish responses without clear communication about their use is that it may result in confusion (Cordner 1998). For example, after one murder in 2013 public concern was expressed that certain CCTV cameras were inoperative throughout Bermuda causing doubt as to the efficacy of their use (Bell 2013a).

Even in todays' society, despite major investments in the criminal justice system, police, courts and correctional facilities, there appears to be little correlation between the increase of money spent on situational crime techniques and crime reduction (Waller and Weiler 1984).

3.3 Social Crime Prevention Theories

Social crime prevention is seen as a secondary type of crime prevention and appears to be in contrast with primary prevention techniques. Social crime prevention seeks to address the wider problems affecting the community and the environment, by altering the aspirations of those at risk of criminality and the way in which they fulfil their goals. Many theorists believe that social crime prevention works better than the more traditional crime prevention methods (Hughes and Edwards 2005).

The aim of social crime prevention is to provide a flexible holistic approach to addressing crime prevention by empowering at risk individuals through social development, education, community building, and comprehensive community improvement (Brown and Richman 1993). Historically, there has been a conflict between the priorities of the community and those of the police, which may be potentially damaging to the relationship (Podolefsky 1984; Meares and Kahan 1998; Winship and Berrin 1999). Some scholars have even suggested that police and community priorities are even more conflicted, because their values are incompatible (Manning 1988, 1993). Very little research has been done to understand this 'value conflict' (Thacher 2001). Although, there may be differences between community and policing priorities, specialist departments, such as Police Community Action Teams (CAT) in Bermuda, have successfully been introduced in order to balance any competing goals and value conflicts (Thacher and Rein 2004). Without maintaining this balance, communities may reject any traditional crime prevention techniques (Podolefsky 1984).

In the case study of a lower class, lower income inner-city area in western Canada, Kelly et al. (2005) aimed to demonstrate that Crime Prevention through Social Development (CPSD) was achievable and sustainable. They demonstrated that urban regeneration is one of the key aspects of being able to sustain any preventative programme (Raco 2007).

However, they employed such a stringent set of criteria when selecting their final case study that success was never really in doubt. Some of the examples of success are briefly discussed in their case-study, but there are no definitive figures, timescales or suitable comparisons to other similar communities as a reference. There is also limited information regarding the involvement of the state, which we presume must have taken place if only to avoid initial financial or legislative concerns (Mohan and Stokke 2000).

The key factor in Kelly et al. (2005) is that the community itself was able to create sustainable funding for the initiative, unlike most 'top-down' government techniques that may be short lived. Social crime prevention therefore requires initial, coordination, government funding or involvement to be successful (Poole 1997).

This community-focused style of policing may mean many things to many people, and as such there isn't an agreed definition for community policing that can be relied upon (Cordner 1998; Mastrofski 1998; Fielding 1995). However, it is generally accepted that central to community policing is the creation of working partnerships between the police, the community and other agencies (Peak and Glensor 1999). These partnerships are considered a priority for police (Rosenbaum 1998), as without the assistance of the community it makes responding to crime more difficult (Moore 1992; Bennett 1998; Bell 2014).

3.3.1 Social Control Theory

The judgement of peers and the community may be more important than that of the enforcement agencies. The Social Control Theory seeks to understand whether anything other than weighing up the rewards against the risks of punishment may affect a decision to commit a crime (Hirschi 1969). Theorists focused on the fact that deviant behaviour is weighed against how much of a stake in conformity the offender risks, balanced against investments made in previous conventional behaviour. Therefore, the individual is less concerned about what punishment the state can enforce, but more what they believe would be lost surrounding their attachments to society (Hirschi 1969: 197). Again when considering this theory against the factors that draw individuals to join gangs or terrorist networks, it becomes an increasingly important theory.

Reckless (1973) further developed the theory arguing that individuals are not only affected by external pressures, but what they desire most at a specific place in time, balanced against their own individual interpretation and understanding of the social bond.

External push-and-pull pressures are extensive and explain why an individual may get pulled into a gang as a way of earning money and achieving status (Reckless 1973). However, this theory may not be appropriate when explaining extreme deviant behaviour (Hamlin 2001). Therefore, it would also be very relevant to discuss whether violent gang-related crime and terrorist acts are examples of extreme deviant behaviour.

3.3.2 Social Learning Theory

Having been developed by Burgess and Akers (1966) to analyse and explain the elements that encourage delinquency versus those that act as a deterrent, the theory suggested that in order to learn criminal behaviour it must first be observed. This theory does help to explain how criminal behaviour can be learnt by observation, and by witnessing the consequences of an action (Bandura and Walters 1963; Bandura 1977). Therefore, while deviant behaviours can be learned, they can also be changed or altered (Carlson 2012: 48). This is where both situational and social crime prevention techniques are able to influence the future behaviour of individuals.

3.3.3 Deviant Behaviour

There are two viewpoints to defining deviant behaviour, the normative perspective and the situational perspective. For most people, committing a crime is considered a violation of generally accepted norms. These norms are generally reinforced by statute, regulations, folkways and moral conduct (Sumner 1906). Therefore, any violation or breach of these common norms is considered ‘deviant’.

However, these perspectives can be eschewed by many different factors e.g. political or legal changes, education, artistic movements, and societal changes as the result of media campaigns (Campaign 2013). Therefore, when an element of criminogenic behaviour becomes more acceptable by society, then over time societal norms may expand to accept that certain type of behaviour (Linton 1955).

Due to the societal causes that may contribute to the gang problem and deviant behaviour, it would appear that the application of social crime prevention techniques may be a more appropriate response. These techniques seek to divert individuals away from gangs by re-educating them, providing them with alternative development opportunities or merely occupying their energy and time (Crabbe 2000). The French Bonnemaison model, which was developed by Gilbert Bonnemaison in 1982 as the result of a response to widespread rioting in cities across France in mid-1991 (Knepper 2007), is considered the epitome of social crime prevention. Rather than placing an emphasis on law enforcement and punishment, governments were encouraged to address the exclusion of certain social groups, the breakdown in community, reduced family values and the absence of leisure activities for young people, all of which may help to divert individuals away from gang membership (Bonnemaison 1992; Knepper 2007). However, depsite the implementation of the Bonnemaison model, the terrorist attacks in Paris (November 2015) highlighted the continued division within French, and ultimately Western, society that may disenfracnhise individuals (Morrison 2015).

Although it was a National Government scheme, the Bonnemaison model had an emphasis on the creation of ‘bottom-up’ social change using local sports and recreation projects (Crabbe 2000). Studies of UK based sports counselling programmes have shown that such prevention techniques can work, thus reducing offending (Nichols and Taylor 1996; Nichols 1997).

4 Research Methodology

The aim of this research is three-fold: firstly, to establish the underlying causes of the increase in gang-related violent crime in Bermuda, and secondly, to determine whether the BPS response to the escalation of gang violence, particularly the implementation of primary crime prevention techniques, effectively reduced gang-related crime. Thirdly, would such techniques be appropriate to prevent future risks affecting Bermuda, such as terrorism.

5 Findings and Discussion

Throughout this research, a number of significant scholarly articles have been discussed that demonstrate that situational crime prevention techniques are effective in reducing crime. However, this paper does not intend to focus on the moral culpability of crimes that do not seem to be affected by situational crime prevention techniques, e.g. drugs and bribery (United Nations 2010).

It is also recognised in this paper that not all murders committed in Bermuda are gang-related.

Analysis of firearms incidents indicates that they may not necessarily be recorded as offences. They are split into 'confirmed reports', (where there is forensic or physical evidence) and 'unconfirmed reports', where there is no evidence to substantiate the report.

By looking at the total crimes recorded (Fig. 1), it is clear that in 2013 they fell below figures recorded in 2004, and are now at their lowest in sixteen years.

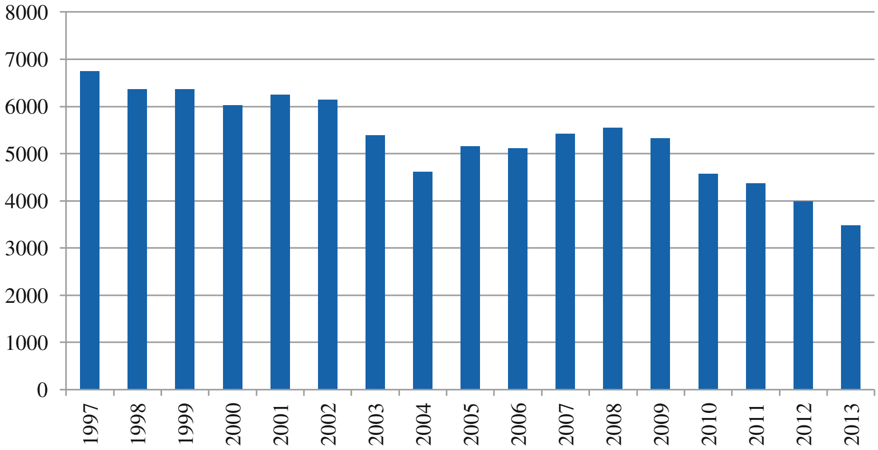


Fig. 1 Total crimes recorded in Bermuda

Although there was a significant decrease from 2001 to 2004, a noticeable rise until 2008 is documented. As a breakdown: from 2001 to 2004 crime declined by 26 %; the four years from 2004 to 2008 saw a 20 % increase in crime, from 4622 crimes, to 5550. There was a small, 3.9 % drop in recorded crime to a figure of 5333 in 2009 (as gang violence and the resultant police activity increased significantly). From 2009 to 2010 a reduction of nearly 800 crimes were recorded. 2011 saw a decrease of 4.5 % on the year before to 4371 crimes. Another significant drop occurred in 2012, when recorded figures dropped below 4000, an 8.7 % decrease on the previous year. Significantly, 2013 saw the crime rate fall 36 % in total from the figure in 2001 (BPS 1998, 2002, 2003, 2006, 2008, 2009a, 2010d, 2011b, 2012c, 2013a, b).

However, while there was a steady decrease of overall crime recorded since 2008, the use of firearms in gang-related violent crime continued to increase exponentially, peaking in 2010 before it too started to decline.

5.1 Assessing the Police Response

There are a number of situational crime prevention techniques that the BPS employed as a response to the increased level of gang activity (that developed in Bermuda since the mid-nineties); this is broken down in the following paragraphs:

5.1.1 Pre-2003

The Police Support Unit (PSU) extensively targeted the developing gangs during their early stages of street-socialisation. The police officers would be deployed to known gang locations to search individuals for drugs, weapons, and to deter anti-social behaviour at locations which were spread throughout Bermuda. There are no official police statistics to record how many stop and searches were conducted prior to 2009 (BPS 2008, 2012d: 18, e).

The Resistance Education and Community Help Unit (REACH) was created in 1996 and utilized five full-time police officers. This was a clear example of partnership policing between the BPS and the Ministry of Education, local schools and families. Due to the success of the initial programme, it was expanded to include all of Bermuda's middle schools, falling under the Gang Resistance Education and Training programme (GREAT) (BPS 1998: 21).

CCTV commenced operations in 1999. The initial wave of cameras brought success in reducing motorcycle thefts in the City of Hamilton (BPS 1998, 1999, 2002), and was used effectively to identify the individuals involved in a significant disturbance on Front Street during 2002 (BPS 2002). Three years after its launch, CCTV was earmarked for upgrade to a digital system, with staff increases to ensure proper monitoring and maintenance (BPS 2002).

In January 2002, the Community Beat Officer Unit (CBO) was created and tasked with focusing on the development of community policing in specific geographic areas. The creation and expansion of the CBO Unit signalled an expansive shift in thinking, embracing the community policing method to improve communication with individuals, communities and other agencies (Greene 2000: 313; BPS 2003).

Also in January 2002, a Firearms Incident Commanders Course was undertaken (BPS 2002) indicating a move towards the adoption of UK policing standards. Furthermore, Bermuda followed the UK's 2001 decision to replace the 16-point fingerprint standard with a non-numerical standard. The Home Office (UK) had determined that the 16-point fingerprint standard had been largely misunderstood during its initial application (Champod et al. 1993), and by adopting the newer standard it allowed greater efficacy in the evidence of fingerprints to detect crime (Buckley 1999 All ER (D) 1521).

In September 2002, school faculties perceived an increase in the 'gang concept' pervading the two public Senior Schools, CedarBridge Academy and Berkley Institute (Bernews 2013a; Jones 2011b). This saw an increase of violence between students. In response, the BPS appointed a Schools Resource Officer (SRO) wherein; the role of the police officer is fused with that of counselor and educator (NASRO 2012).

5.1.2 2003

One person was shot and killed in what was described as one of the catalytic moments in the sudden rise of gang-violence (Strangeways 2011a). Police operations were on going throughout the year and in December 2003 Operation Zero Tolerance was put into operation and targeted the top twelve '*crack houses*' and '*hotpots*'.

5.1.3 2004

While there was a slight rise in confirmed firearms incidents in 2004, there were no recorded murders or injuries associated with gangs and their use of firearms. A pistol was brandished at police on Court Street, however no one was hurt. Gang violence continued to occur with violence erupting at sporting events. The only murder during the year was domestic related. However, due to the increasing gang-violence the US Government issued a travel advisory warning to their citizens (Wells 2004).

The refurbishment of the BPS firearms range in 2004 allowed for an increase in training of officers in the use of police firearms and tactics, and the Emergency Response Team (ERT) was able to return to full strength. At the time the ERT was the primary response to firearms threats and the officers had to be called in from other duties each time they were required.

5.1.4 2005

Compared to previous years, 2005 saw a significant rise in firearms offences, although no gang-related murders were committed. Natural wastage of police officers occurred, a reduction of almost 22 % of the established officer strength (BPS 2006). This reduction in manpower may have contributed to the rise of crime during this period.

5.1.5 2006–2008

Overall crime rose sharply between 2006 and 2008 while firearm offences actually fell. There was an increase in gang-related murders committed with one and two murders being recorded in 2006 and 2007 respectively. The second murder of 2007 occurred on Boxing Day; two other men were shot and injured during this incident. This particular incident began to highlight the gang problem, which had slowly been escalating out of control (The Bermuda Sun 2007). As a result of the Boxing Day shootings in 2007, the BPS publicly outlined a perceived a common trend, with witnesses and victims failing to cooperate with police investigations.

An important development within the BPS occurred at this time as a response to the increased number of gang-related firearms incidents. Since the 1st of January 2008, Bermuda has seen a permanent presence of armed police on the streets in the form of Armed Response Vehicle Teams (ARVs). The creation of this unit allowed for armed police officers to be more easily deployed to increasing gun and gang violence incidents (BPS 2008).

Furthermore, the BPS implemented Operation Safer Streets (OSS) on the 4th January 2008. Operation Safer Streets was a crackdown by the BPS on known hot spots. During the initial phase of this crackdown there were 87 arrests, 99 residential and street searches were made under the Misuse of Drugs Act 1972, five firearms warrants were executed and six bladed articles were seized (BPS 2010a).

None of the murders in 2008 were associated with gang or gun violence. However, Bermuda's crime and murder rate (per capita) was increasing and being highlighted in the press (Hall and Gibbons 2008; Palmer 2008; Wells 2008).

A comparison of the 8962 arrests carried out between 2003 and 2007 shows that males accounted for 88 %. Furthermore, 70 % of those arrested during the five-year period were black, 15 % were white and 22 % were Portuguese, with the remainder recorded as unclassified (BPS 2003, 2006, 2008). As a result of OSS, total arrests for 2008 were 3255, almost doubling the figures from 2007 (Department for National Drug Control 2007). This provides an initial tentative suggestion that the increase in police proactivity may have caused the decline in murders but that the total crime remained high, as a result of the increased detection of connected factors at the time, such as drugs and anti-social behaviour (Sherman et al. 1997; Gurr et al. 1977: 93–96, 140; Wilson and Kelling 1982).

Another long-term development was the implementation of the Police and Criminal Evidence Act 2006 (PACE) on the 7th September 2008. This outlined the legal powers and policies of police stop and search procedures and increased the transparency and accountability of police operations to the community. It also changed the arrest policy for any offence that carried a conviction penalty of three months imprisonment to an automatically arrestable offence (PACE 2006). Again, this may have caused the increase in arrest data during this period (BPS 2008).

Police stop and search has always been a contentious part of policing (Melathe 2014), and has been cited as negatively impacting public confidence in the police (Miller et al. 2000; Delsol and Shiner 2006).

Prior to the implementation of PACE in Bermuda, the BPS had been criticized for being insensitive in the handling of individuals (Criminal Justice Review Team 1992). This initial lack of policing awareness may have caused the lack of cooperation or trust from the community during early gang-related crime investigations (Podolefsky 1984).

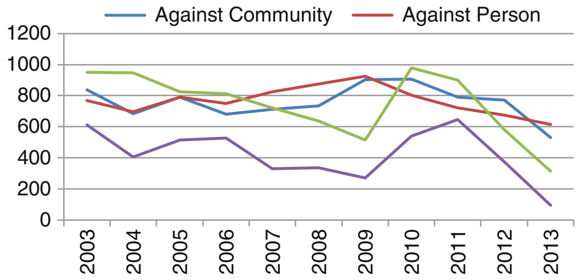
5.1.6 2009

Total crime decreased by 3.9 % in 2009, when compared to 2008. However, 'crimes against the person' and 'crimes against the community' increased by 6.2 % and 22.3 % respectively (see Fig. 2). This rise may be explained by significant rises in firearm offences and anti-social behaviour, which had tripled from the first to the fourth quarters of 2009 (BPS 2009a).

The BPS further targeted the individuals that presented an increased concern to the community (Farrington 1992: 534; Wyrick 2006). Arrest figures increased in 2009, by a further 1300 arrests from the year before. In the first three quarters of 2009 there were more arrests made than in the whole of 2008. October 2009 saw the BPS realign the Service to ensure that there was an 85 % shift of officers to operational policing, and the creation of a dedicated gang targeting team (BPS 2010c: 1).

The first of the murders in 2009 occurred on the 22nd May. Kewandee Robinson was shot in broad daylight on St. Monica's Road (42 Gang area) and had its foundations in the on-going feud between 42 and Parkside. Bermuda had not seen a fatal shooting since the 26th December 2007. During 2009 six persons were murdered, four of which were attributed to gang-violence. Reprisal shootings

Fig. 2 Fluctuating Crime Figures: *Source* BPS quarterly statistics



increased throughout the year, and as a result thirteen individuals were also wounded by gunfire (BPS 2009a).

The number of arrests in 2009 also rose by approximately 40 %. The final two quarters of that year saw arrest rates almost double that of the first two quarters. Significantly, police stop and search incidents also steadily increased throughout 2009. The final quarter saw the highest number of stop and search incidents conducted, with 1354 being carried out; a 68.4 % rise occurred in the third quarter. One explanation for this steady increase may have been the introduction of new police powers (PACE 2006; BPS 2009c: 19, 2010). Another explanation may be due to the increased street presence of the police. There are no stop and search figures recorded prior to 2009 to compare (BPS 2008).

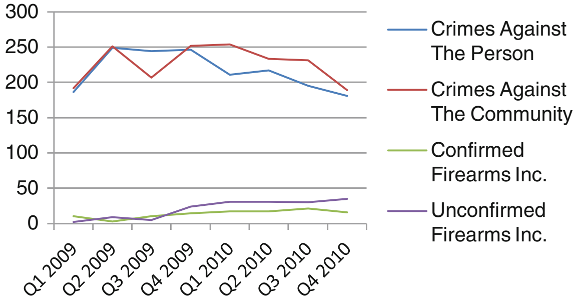
5.1.7 2010

During 2010 the escalation of violence continued, with seven people murdered and twenty-nine people injured. 2010 was without a doubt the worst year in Bermuda's history for gang-related violent crime. Several high profile murders took place that shocked the Island and appeared to suggest that the police had lost control; a triple shooting on Court Street (YouTube 2014) and the daylight shooting of Kimwande Walker at a community event that was attended by dozens of children (Jones 2010a, b; Bernews 2010).

Overall crime fell during Q1 2010 to the lowest since the same quarter in 2006, in complete contrast to the increase of gang violence, which was now spilling into everyday community events. The first quarter of 2010, saw a further increase of firearms incidents (confirmed and unconfirmed). Total firearms incidents had risen 72.5 % over the first quarter in 2009. This figure suggests that the situation had spiraled out of control, but may also suggest that the community were reporting incidents more willingly. This second explanation appears to be more reasonable when comparing the unconfirmed firearms incidents, which also increased exponentially along with calls for service as overall crime rates began to fall. A dramatic rise of 45.83 % in the reporting of these incidents occurred in Q1 2010 (BPS 2010d) (Fig. 3).

In early 2010, the Federal Bureau of Investigation (FBI) Safe Streets and Gang Unit visited Bermuda and provided training. Also in 2010 the BPS recruited a new

Fig. 3 BPS quarterly figures for 2009 and 2010 (BPS 2010d)



Assistant Commissioner of Police from the West Midlands Police (UK), who had been at the forefront of dealing with gang violence in Birmingham in the preceding decade (Jones 2010a, b; The Bermuda Sun 2010). At the same time, experienced Authorised Firearms Officers (AFOs) were recruited from the UK to bolster numbers in the ARV Units (Close Protection World 2010).

Tasers were also introduced in 2010, six years after their introduction in the UK, and were considered an appropriate response to combat the risks that officers had started to face on the streets (BPS 2010b). Stop and Search initiatives were a third greater during 2010 than they were in 2009, with arrests increasing further by over 500 from the 2009 figures (BPS 2010d).

5.1.8 2011

There was very little respite in killings in 2011 when a 29 year-old man was shot dead in Somerset Parish. However, the victim may have had no gang affiliation (The Royal Gazette 2011a). Although 2011 saw a fall in gang-related violence, by the end of July there had been 27 'confirmed firearms incidents' resulting in five murders and four others injured. This demonstrates a slowing of confirmed incidents against the previous year, when six persons had been murdered and fourteen persons injured in the same period (BPS 2011f). In the second half of 2011 eleven persons were shot and injured (Royal Gazette 2011b).

During this year, the murder rate became double the world average (Strangeways 2011d). 63 % of murders during this period were committed using a firearm and 75 % of the (total) murder victims were aged between 20 and 29 (Her Majesty's Inspectorate of Constabulary 2012).

The fact that 75 % of murder victims recorded in 2011 are in the age group of 20–29, which represents 12 % of the population in Bermuda (Strangeways 2011d), indicates that there is a strong basis for the argument that young men perpetrate the majority of gang violence. It also appears to lend weight to the premise outlined in the introduction that young male members of society are responsible for the increase in crime (Fig. 4).

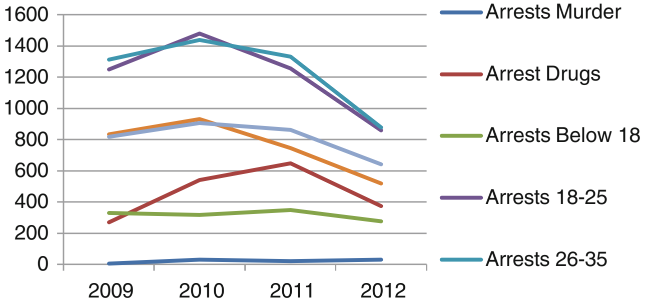


Fig. 4 Arrest data based on age (BPS 2009b, 2010d, 2011b, 2012c)

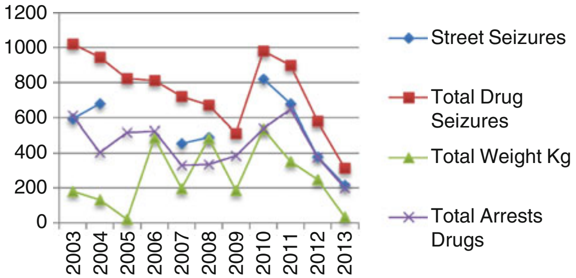


Fig. 5 Although data is missing, there are significant rises in all categories of activity in 2009 and 2010, followed by rapid decline. *Source* BPS quarterly statistics

Other significant measures that emerged during 2011 were the electronic tagging of offenders (Scott 2011), the creation of an Inter-Agency Gang Task Force (Wilson 2012b) and a witness protection scheme (Strangeways 2011e).

In the three years preceding 2011, the number of calls to the police escalated by 38 %, demonstrating a possible increased concern and willingness to assist the police (BPS 2012b).

Drug enforcement activity is a crucial factor in combating gangs (Fig. 5) (BPS 2010a, 2011b). A spike in activity in 2005 and 2006 accompanied a drop in enforcement activity in 2007 and 2008, to below the average. This then rose significantly in 2009 to the first quarter of 2010, when it doubled from the same quarter of 2009.

5.1.9 2012

This year saw reductions in all areas of crime. Overall crime was down by 8.7 % from the year before and although 2012 saw a decrease of firearms incidents, the number of murders remained the same as the previous year. The number of injuries as the result of gang-related firearms offences also dropped to seven. The final murder of 2012 occurred on Christmas Day on St George's Golf Course (BPS 2012c).

5.1.10 Summary of 2009–2012

Between the spring of 2009 and the end of 2012, over 300 gang-related shootings had been recorded, with more than 70 people injured, some seriously, and 21 men had lost their lives (BPS 2012a). Although 2009 saw a massive increase in the rise of police operations, stop and search, arrests, drug enforcement and drug seizures, 2009 also saw an increase in gang-related violence. This heightened police activity continued throughout 2010 before steadily declining in the following years, corresponding to falls in crime overall.

5.1.11 2013

In early 2013, a double murder occurred on Happy Valley Road, Pembroke, in what was believed to have been an MOB attack. The remainder of 2013 saw two men stabbed to death in non-gang-related incident, and another gang member was shot and killed (Bernews 2013b).

The implementation of Bermuda's own Operation Ceasefire in the middle of 2013 was heralded as the next development in the fight against gang-related violence (Strangeways 2013). Operation Ceasefire was successfully implemented in Boston, as an interagency problem solving initiative that was initiated as a response to the increase in youth gang murders between 1991 and 1995 (Braga et al. 2001; Butterfield 1996; Witkin 1997), and was initiated with a realization that the violence was driven by a small group of young male recidivists.

5.2 *Theory Testing*

This study has focused on the period between 2003, when the first gang-related murder involving the use of a firearm was recorded in Bermuda, and the end of 2013.

The *per capita* data presented in the following chapters has been calculated using the approximate population figure of 64,000, which was obtained during the last census in 2010. However, the population may have increased to around 61,500 since the last count of the population (Department of Statistics 2010; Kowalski 2013; Government of Bermuda 2013).

In the first six years, 31 % of the murders were gang-related. This is slightly higher than the gang murder rate in Canada at that time which was around 25 % (Beattie 2009). This increased significantly to around 77 % (Fig. 6), likening it to gang-related murder rates in some large US cities (National Gang Center 2011).

Without gang-related murders there would have been 18 murders recorded in this time period. Therefore, when gang-related murder is discounted, Bermuda's average murder rate per capita for the eleven years would be 2.6 per 100,000 population (Fig. 7).

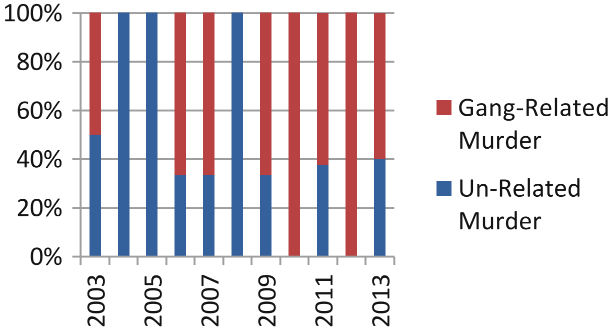


Fig. 6 Murder percentages. *Sources* Government of Bermuda (2013)

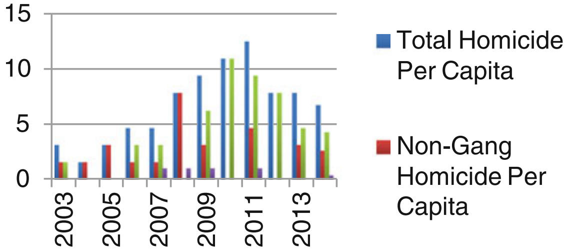


Fig. 7 Graph displaying yearly total, non-gang and gang-related murder rates per capita based on a population of 100,000

Notable differences in these figures occurred in 2008, and in 2010. Furthermore, in 2011, the murder rate per capita rose to 12.5, the highest recorded in Bermuda's recent history.

Therefore if we discount gang-related murder figures during the years of study, then the 2008 figure, which is 7.81 (the highest recorded annual figure), appears to be an anomaly. Even with this high 2008 figure, the average murder rate for non-gang-related murder for the decade is 2.6 per capita, which actually moves Bermuda into the top 75 countries with the lowest murder rates (United Nations 2012b). Notably, there were no murders recorded (other than gang-related) throughout 2010 and 2012.

However, when gang-related murders are incorporated, the total average murder rate per capita for the decade increased to 6.7 and takes Bermuda to a position of 115 out of 196 in the international league table for murders per capita (United Nations 2012b), supporting the earlier theory that young black men who are associated with gangs contribute significantly to violent crime in Bermuda (Fig. 8).

Interpreting the collected data during this research may start to support the early assumptions regarding the actors, the initial causes of gang-related violence and the subsequent reduction of crime in Bermuda. However, remembering the premise that situational crime prevention techniques may not be effective in reducing violent crimes or crimes of passion (Geason and Wilson 1988), then prior to presenting a concluding argument it is essential to conduct theory testing surrounding the data.

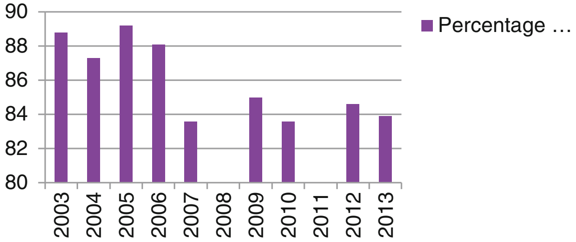
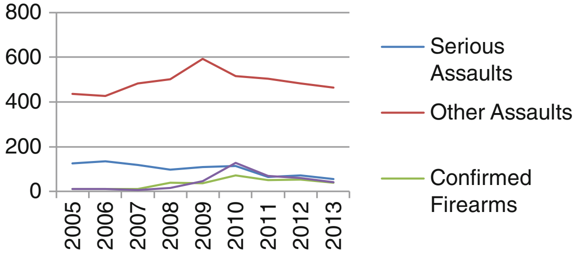


Fig. 8 Percentage arrests for males. *Source* Bermuda Police Service

Fig. 9 Crimes against persons



5.2.1 What Caused the Outbreak of Violence?

It is already understood that there were a number of events that occurred in the early part of the decade that have been described as catalysts for gang-related violence. However, can probability testing support these assumptions (Fig. 9)?

Tests of correlation were conducted to compare the rise of ‘serious assaults’ from 2005 to 2010 against ‘total crime’. There was a strong positive correlation suggesting that violent crime and crime had a direct relationship with one another. There was a negative correlation between ‘serious assaults’ from 2005 and ‘total arrests’, but this was not significant. Therefore as arrests rose, serious assaults fell.

5.2.2 Did Police Actions Affect Crime?

Initially, two continuous variables from the data analysed the relationship between ‘total arrests’ and ‘total crime’ for the period. Correlation tests demonstrated that there was a weak, negative correlation between these variables and this relationship was statistically significant. This suggests that as total arrest figures increased, total crime figures fell. Although a weak negative correlation, it demonstrated that increased police arrests had an effect on reducing ‘overall crime’. As arrests were significantly lower than total crime in the first half of the decade the correlation appears to be positive. However in 2009, after police restructuring, we can see that a negative correlation occurs (crime falls as arrests figures rise). The rise in arrest figures then levels out before both sets of figures fall. Arrests remained higher than crime in 2010 and 2011, before declining below ‘overall crime’ in 2012 and 2013.

In order to further investigate the possibility of police arrests affecting crime figures, the decade was split in half. Further tests were then conducted. ‘Total arrests’ were compared against ‘total crime’ from 2003 to 2008. This showed that there was a weak positive correlation. However, the result is not significant. The data from 2009 to 2013 was then compared demonstrating that there was a strong positive correlation with little significance (Fig. 10).

The relationship between ‘stop and search’ and ‘total arrests’ was also analysed and a moderate positive correlation between the variables was seen, and this was not statistically significant. This demonstrates that as the number of ‘stop and search’ increased so too did the number of arrests. This appears to reflect the

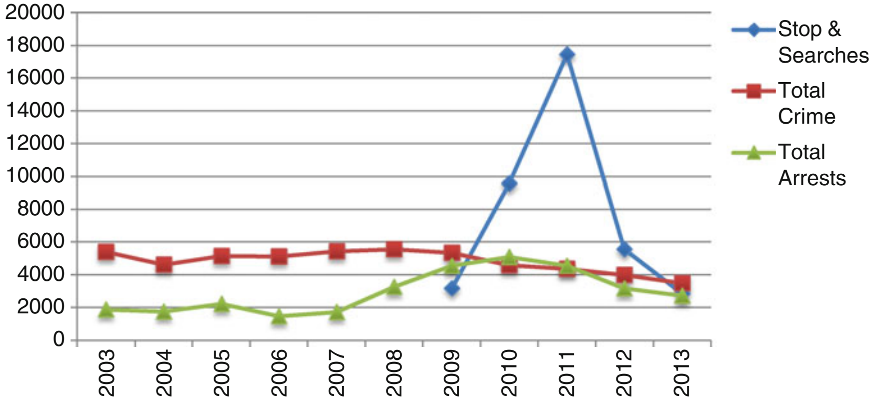
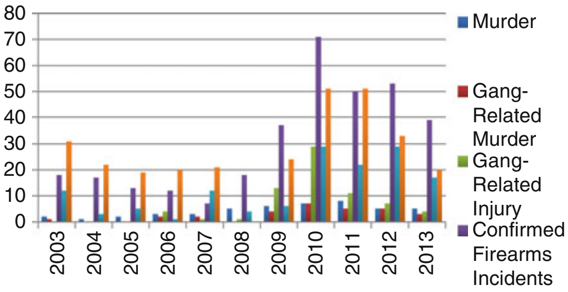


Fig. 10 Compares stop and searches by police, total crime recorded and total arrests for the decade. N.b. no stop and search data is available before 2009

proactive nature and changes to the structure of the BPS at the time. Arrest data covering 'gang-related murder' and 'murder' demonstrated a strong positive correlation between the variables and the relationship was statistically significant, suggesting that as gang-related murders increased, so did police activity (Fig. 11).

The relationship between 'gang-related murder' and 'confirmed firearms incidents' showed a strong positive correlation between the variables and the relationship was extremely statistically significant. Further confirming that as an increase in firearms incidents occurred so too did the number of gang-related murders. This may be a relevant factor when trying to determine the possibility of future increases in gang-related violence, as discussed later. 'Gang-related injury' and 'confirmed firearms offences' were also analysed. There was a strong positive correlation between the variables and this result was extremely significant. This continues to support the theory that firearms activity relates directly to gang-violence. 'Confirmed' and 'unconfirmed' firearms incidents were also tested (from 2006 to 2013). There was a strong positive correlation between the variables and this result was significant. Again, following from the previous two tests, there appears to be a statistically significant connection between the two.

Fig. 11 Only partial data for 2008 was available



The same tests were performed between ‘gang-related murder/injury’ and ‘unconfirmed firearms incidents’ to see if the results could be further supported. These were performed from 2006 to 2013 due to unavailable data in previous years. Between ‘gang-related murder’ and ‘unconfirmed firearms offences’; a strong positive correlation between the variables exists and the result was significant. Similarly, gang-related injury (from the use of a firearm) and unconfirmed firearms incidents; dsiplayed a strong positive correlation between the variables and is also considered significant.

Having conducted further tests of correlation it is possible to suggest that this relationship of data may be used as an early warning to police. If a sudden increase of firearms incidents were to occur, then several reasonable assumptions may be made, and a gang-related murder or injury may be imminent, and thus preventable. Can these theory tests also support the assumptions that an increase of police stop and search affected the rising crime trends at the time?

Further tests of correlation were undertaken between different variables and although there were weak correlations between them, none were thought to be particularly significant and therefore required no further discussion.

6 Conclusion

Gang-related violence is a security threat in Bermuda. This study has attempted to discover whether the responsiveness of the BPS has had a significant impact on crime in Bermuda. The results compiled have shown that this may be the case, although significant reduction were only recorded in 2012 and 2013. This could have resulted from the changes in policing policies instituted in 2009 that shifted the focus to frontline policing and impacted on overall crime in a very significant manner. This phenomenon is known as the ‘bonus effect’ of situational crime prevention techniques (Sherman 1990) where extra positive effects are derived from the methods, above and beyond the reasons for their initial application. Other criminologists have labeled this the ‘halo effect’ (Scherdin 1986) or the ‘free rider effect’ (Miethe 1991).

This ‘effect’ was not felt between the years 2007 and 2010 as pertaining to gang-related violence, firearms offences and gang-related murders which continued to increase with reliable regularity (BPS 2010d, f). However this does not render the methods ineffective, more simply, they were a work in progress. The combination of situational crime prevention techniques and social crime prevention techniques would eventually have a significant effect on reducing violent crime.

There is clear historical evidence of proactive policing in the years leading up to the sudden outbreak of gang-related violence in 2009 through police crackdowns and school interventions, an inability to successfully convict suspects of murder, an apparent unchecked rise in crime and violence may have encouraged deeply entrenched social problems to manifest. It would therefore, be hard to lay any fault at the feet of the BPS. In fact, it is reasonable to suggest that the apparent failure of society and the criminal justice system to respond accordingly to the violence throughout the twentieth century may have indeed led to societal acceptance/ ignorance of the violence in the early part of the decade (Comeau 2012). The reaction of society to violations and the severity of those violations may vary amongst communities (Black 1976), but they may encourage violations of social norms to increase over time (Hirschi 1969). This can be reasonably demonstrated by the fact that in the four years leading up to 2009, almost 10 % of the population had been arrested and recidivism rates were high with at least 42 % of prisoners reoffending. Although this figure was down from 78 % the year before, new recording methods had been implemented which may have had a bearing on the figures. Furthermore, due to these societal failings, young men who are 'at risk' may still join gangs in an effort to fulfill their needs (Maslow 1943; Comeau 2012; Broadhurst et al. 2005).

Ironically, while crime is generally considered a divisive force, this crescendo of gang-related violence may have in fact strengthened community bonds (Durkheim 1933). The increased sharing and reinforcing of conventional values through political and religious participation, community action groups, Neighbourhood Watch schemes, media reporting and greater community partnerships may have accelerated during this decade as a societal reaction to the outbreak of gang-related violence (Garofalo and McLeod 1986).

Coupled with studies of crime-affected neighbourhoods that suggest that a fear of crime alone can undermine trust and support in the police (Skogan 1986) and that community schemes are lacking where they are needed most (Garofalo and McLeod 1986; Schoenberg 1983), then it is reasonable to suggest that certain social issues had become entrenched in the fabric of society. However, in 2013 the Police Commissioner announced that collaborative efforts between the police and community partners were finally bearing fruit after several years of effort.

As to whether the action by police had any effect on crime figures, can be answered by examination of the results. The theory testing results demonstrate that total arrests affected total crime for the decade. A positive correlation was found between the two halves of the decade and a negative correlation for the decade as a whole; this final correlation was statistically significant. This supports earlier assumptions how arrests may have affected crime. If a positive correlation had been found for the whole decade, then there may be grounds to suggest that total arrests rose as a reaction to crime. While this may have been the case in the first half of the decade, there is clear evidence that arrests increased higher than crime in 2010 and 2011 and as a possible result, crime fell.

This fall in crime does not appear to be the result of chance due to the fact that Operation Safer Streets started at the beginning of 2008 and ran throughout 2009. The arrest figures rose steadily throughout both of these years, demonstrating that situational crime prevention had a reduction effect on crime. Despite, the criticism that situational techniques may lack permanency, the BPS restructured their resources in 2009 placing more emphasis on frontline policing to ensure sustainability (BPS 2010c: 1).

The BPS actualised a multitude of crime prevention techniques in order to tackle gangs. These included improved investigation techniques and heightened proactivity focusing on prolific offenders, the enforcement of new crowd dispersal legislation (Wilson 2012a); over $1 m seized under the Proceeds of Crime Act 1997 (Wilson 2013a), high-visibility policing during holiday periods (Wilson 2013c), use of covert techniques to increase intelligence on offenders, and partnership approaches to tackle the social issues of those considered 'at risk'; increased officer training, gun bounty schemes (Wilson 2013b), cold case specialists hired (Stevenson 2014; Jones 2011a; Roberts 2009), a DNA database (Roberts 2009), increased prison sentences (Bell 2013b; Dickey and Hollenhorst 1999), electronic tagging, and a greater investment in tackling entrenched beliefs through involvement in schools and sport (Smith 2013).

This study focuses on the situational crime prevention tactics that were employed by the BPS and whether they had any effect on reducing gang-related violent crime in Bermuda. What emerges is that the use of social crime prevention alongside situational techniques is essential. However, while social prevention schemes are now becoming more established, it would be wise to ensure that the focus remains on those individuals most 'at risk' of joining gangs, and not be side tracked by other issues such as general juvenile delinquency (Esbensen 2000; Battin-Pearson et al. 1998). Having mentioned that similar drivers exist between those individuals that join gangs and those that join terrorist networks, more intrusive research into the gangs, or those youths most at risk would be desirable in the future. This further supports recommendations that 'lone wolf terrorists' that become indoctrinated, may just be saddened individuals who wish to cause harm, and that such individual's actions are determined by social inadequacy and society's '*failure to give meaning to people's lives*' (Furedi 2012; Wilson 2013d), and that a more systematic approach when forecasting terrorism and terrorist networks is required. The comparisons between gangs and terrorist organisations are strikingly similar and require much more coordinated research.

Furthermore, localised displacement of gang-related crime would also benefit from more focused statistical scrutiny. There is evidence in this research to suggest that there has been a diffusion of crime control benefits (Clarke and Weisburd 1994) as figures for overall crime have steadily fallen despite gang-related violent crime fluctuating. Yet no empirical studies of displacement in Bermuda could be found.

There is also little empirical evidence in Bermuda surrounding the involvement of gang members in crime. While there is evidence to suggest that youth gang-members are responsible for a higher rate of offending than non-members, little statistical data is available to understand the problem in Bermuda. However, if this data were available it may be able to explain the occurrence of between three and twenty-five times the amount of crime that gang-members are understood to commit (Howell 1998, 2010).

Without adequate mapping of crime or ethnographic studies, less is known about the effects of the crime prevention strategies. The crowd control dispersal legislation used by the BPS prior to 2012 is a prime example of successful situational crime prevention. However without the correct recording and analysis of the results, it is not possible to fully measure the effect. Furthermore the importance of these possible research findings cannot be discounted as gang-related violence in the Caribbean has increased substantially within the past decade, while other areas of the world have seen a fall or at least a stabilization of gang crime (United Nation 2012a). There is a clear opportunity for further research being used for international cooperation in reducing gang-crime or terrorism in other jurisdictions, the Cayman Islands for example (Cayman News Service 2013; Whittaker 2013; Fuller 2010; Robbins 2010).

In the grand scheme of the overall problem facing society, focusing on such small jurisdictions may seem arbitrary, nevertheless it is proposed that it would allow for greater focal intensity on the methodology of the research, which could be implemented on grander scales. With more intrusive, consistent and analytical research between similar jurisdictional partners that share comparable geographic, topographic and societal values, a greater understanding of ethical, adaptable and sustainable crime prevention techniques can be established in order to combat violent crime. With a deeper understanding of this problem, such techniques may then be applied to the threat of global terrorism and violent extremism. After all, the warning signs appear to be present in Bermuda; socioeconomic and political grievances resulting in motivation for individuals (Cragin 2007: 9), disaffected and socio-uncohesive youth, terrorist ideoliolised graffiti; possibly as a result of the saturation of extremist ideology via social media (Kimery 2015). Also a possible lack of imagination by the authorities (Corbin 2003), or ignoring clear warning signs or specific behaviours (Borum *et al.* 2004: 428; Reich 1998) that lead to the sudden increase of gang-related violence could also lead to an emergence of a terrorist threat.

Although it is impressive what such a small police service with limited resources, was able to achieve in such a small time frame. Without *any* continuing statistical scrutiny it is impossible to state whether these techniques may be suitable in reducing gang-related violence and whether Bermuda is adequately posed to manage emerging security threats in the future.

References

Bakker E (2006) Jihadi terrorists in Europe. Their characteristics and the circumstances in which they joined the Jihad: an exploratory study. Netherlands Institute of International Relations, Clingendael

Bandura A (1977) Social learning theory. Prentice-Hall, Oxford

Bandura A, Walters RH (1963) Social learning and personality development. Holt, Rinehart, and Winston, New York

Battin-Pearson SR, Thornberry TP, Hawkins JD, Krohn MD (1998) Gang membership, delinquent peers, and delinquent behavior. Department of Justice, Office of Juvenile Justice and Delinquency Prevention Bulletin. Youth Gang Series. Washington, DC

BBC (2006) What do you think of Nigeria? BBC News. Online forum, 16 June 2006. Accessed 2 Dec 2013

BBC (2009) Global recession timeline, BBC News. 09 September 2009. Available from http://news.bbc.co.uk/2/hi/8242825.stm. Accessed 12 Oct 2013

BBC (2010) Nigeria ethnic violence “leaves hundreds dead”, BBC News. 03 August 2010. Available from http://news.bbc.co.uk/1/hi/world/africa/8555018.stm. Accessed 10 Dec 2013

Beattie, S (2009) Murder in Canada, 2008. Juristat 29(4). Statistics Canada Catalogue no. 85-002-XIE, Ottawa

Bell J (2013a) Francis aims to build pride in Cedarbridge. RoyalGazette.com, 7 March 2013. Accessed 6 Dec 2013

Bell J (2013b) Police to get islandwide CCTV network. RoyalGazette.com, 20 Sept 2013. Accessed 13 Sept 2013

Bell J (2014) Crime down, RoyalGazette.com. Accessed 29 Jan 2014

Bennett T (1998) Police and public involvement in the delivery of community policing. In: Brodeur JP (ed) How to recognize good policing: Problems and issues. Sage and Police Executive Research Forum, Thousand Oaks

Bermuda Government (2013a) The future of Bermuda’s exclusive economic zone. Outcome of the Public Consultation September 3 to October 31, 2013. Sustainable Development Department

Bermuda Government (2013b) Emigration: Bermuda’s qualified human capital departs: a 2010 census analytical brief by the Department of Statistics, Jan 2013. Available from http://www.gov.bm/portal/server.pt/gateway/PTARGS_0_2_980_227_1014_43/http%3B/ptpublisher.gov.bm%3B7087/publishedcontent/publish/cabinet_office/statistics/dept___statistics___additonal_files/emigration_brief_0.pdf. Accessed 10 Sept 2013

Bermuda Police Service (1998) Annual report 1998. The Bermuda Press. Available from http://www.bermudapoliceservice.bm/upload/PDFs/PoliceAR1998.pdf. Accessed 3 Aug 2013

Bermuda Police Service (1999) Annual report 1999, The Bermuda Press. Available from http://www.bermudapoliceservice.bm/upload/PDFs/PoliceAR1999.pdf. Accessed 3 Aug 2013

Bermuda Police Service (2002) 2002 annual report—Bermuda police service. Bermuda Press Limited, Bermuda

Bermuda Police Service (2003) 2003 annual report—Bermuda police service. Island Press Limited, Bermuda

Bermuda Police Service (2006) 2005/2006 Annual report

Bermuda Police Service (2008) 2007/2008 Annual report

Bermuda Police Service (2009a) BPS crime statistics (Q4 2009)

Bermuda Police Service (2009b) Quarterly crime statistics—4th Quarter 2009 (01-October-2009 to 31-December-2009)

Bermuda Police Service (2009c) Quarterly crime statistics—3rd quarter 2009 (01-July-2009 to 30-September-2009)

Bermuda Police Service (2010a) Gang and violence reduction strategy (GVRS). Bermudapoliceservice.bm. 14 Sept 2010

Bermuda Police Service (2010b) ‘Introduction of taser’, Bermudapoliceservice.bm, press release, 21 April 2010. Available from http://www.bermudapoliceservice.bm/node/2474. Accessed, 1 Sept 2013

Bermuda Police Service (2010c) Annual policing plan 2010

Bermuda Police Service (2010d) Crime statistics report (Q4 2010 and Year End 2010)

Bermuda Police Service (2010e) Quarterly crime statistics—Q2 2010 (01-April-2010 to 30-June-2010)

Bermuda Police Service (2010f) Quarterly crime statistics—Q1 2010 (01-January-2010 to 31-March-2010)

Bermuda Police Service (2010g) BPS crime statistics (Q1 2010)

Bermuda Police Service (2011a) Community spirit grows at Friswells Hill Clean Up Day. The Bermuda Sun, press release. 25 Aug 2011. Available from http://bermudasun.bm/Content/NEWS/News/Article/Community-spirit-grows-at-Friswells-Hill-clean-up-day/24/270/53855. Accessed 12 Jan 2014

Bermuda Police Service (2011b) BPS crime. Statistics Q1:2011

Bermuda Police Service (2011b) Quarterly crime statistics 2011 (Q4 2011 and Year End 2011)

Bermuda Police Service (2011c) Quarterly crime statistics, Q3 2011 (01-July-2011 to 30-September-2011)

Bermuda Police Service (2011d) Quarterly crime statistics, Q2 2011 (01-April-2011 to 30-June-2011)

Bermuda Police Service (2011e) Quarterly crime statistics, Q1 2011 (01-January-2011 to 31-March-2011)

Bermuda Police Service (2012a) Overall crime stats fall in 2012, RoyalGazette.com, Available from http://www.royalgazette.com/article/20130227/NEWS03/702269908. Accessed 2 Feb 2014

Bermuda Police Service (2012b) 'November 21—daily report', Media Relations Dept., 20 Nov. 2012. Available from http://www.bermudapolice.bm/report_view.php?n_id=3806/. Accessed 3 Aug 2013

Bermuda Police Service (2012c) Quarterly crime statistics 2012 (Q4 2012 and Year End 2012)

Bermuda Police Service (2012d) Quarterly crime statistics, Q2 2012 01-April-2012 to 30-June-2012

Bermuda Police Service (2012e) Quarterly crime statistics, Q1 2012. 01-Jan-2012 to 31-March-2012

Bermuda Police Service (2013a) Quarterly crime statistics, Q2 2013 01-April-2013 to 30-June-2013

Bermuda Police Service (2013b) Quarterly crime statistics, Q1 2013 01-January-2013 to 31-March-2013

Bernews (2010a) BDA: not a back of town or black mans problem, Bernews, 3 Apr 2010. Available from http://bernews.com/2010/04/bda-not-a-back-of-town-or-black-mans-problem/. Accessed 2 Sept 2013

Bernews (2010b) Chart: firearms stats for 2005–2010, Bernews, 1 Dec 2010. Available from http://bernews.com/2010/12/chart-firearm-stats-for-2005-2010/. Accessed 2 Sept 2013

Bernews (2010c) 39 unsolved murders, deaths and disappearances, Bernews, 23 Mar 2010. Available from http://bernews.com/2010/03/list-bermudas-unsolved-murders-disappearances/. Accessed 2 Sept 2013

Bernews (2010d) Murder victim: troy "Yankee" Rawlins, Bernews, 9 Aug 2010. Available from http://bernews.com/2010/08/murder-victim-troy-yankee-rawlins/. Accessed 2 Aug 2013

Bernews (2011a) Murder trial: Antonio Myers found guilty, Bernews, 28 Mar 2011. Available from http://bernews.com/2011/03/murder-trial-antonio-myers-found-guilty/. Accessed 2 May 2013

Bernews (2011b) Parkside gun used in numerous shootings, Bernews, 24 Mar 2011. Available from http://bernews.com/2011/03/parkside-gun-used-in-numerous-shootings/. Accessed 2 May 2013

Bernews (2013a) CedarBridge academy's Graffiti control program, Bernews, 31 Jan 2013. Available from http://bernews.com/2013/01/cedarbridges-academys-graffiti-control-program/. Accessed 6 Dec 2013

Bernews (2013b) Police identify murder victim as Jonathan Dill, Bernews, 3 Sept 2013. Available from http://bernews.com/2013/09/police-identify-murder-victim-as-jonathan-dill/. Accessed 3 Sept 2013

Black D (1976) The behavior of law. Elsevier Science and Technology Books

Block CR, Block R (1993) Street gang crime in Chicago. National Institute of Justice (NIJ), U.S. Department of Justice (USDOJ), Washington

Blumstein A, Wallman J (2000) (eds) The crime drop in America. Cambridge University Press, New York

Bonnemaison G (1992) Crime prevention: the universal challenge. In: McKillop S, Vernon J (eds) National overview on crime prevention. Austalian Institute of Criminology, Canberra

Borum R, Fein R, Vossekuil B, Gelles M, Shumate S (2004) The role of operational research in counterterrorism. In: Mental health law and policy faculty Publications. Paper 324. http://scholarcommons.usf.edu/mhlp_facpub/324

Braga AA, Kennedy DM, Waring EJ, Piehl AM (2001) Problem-oriented policing, deterrence and youth violence: an evaluation of Boston's operation ceasefire. Journal of Research in Crime and Deliquency, 38(3):195–225.

Briggs R (2005) Invisible security: the impact of counter-terrorism on the built environment. In: Briggs R (ed) Joining forces: from national security to networked security. Demos, London, pp 68–90

Broadhurst K, Duffin M, Owen K, Gill M (2005) Research into the views and perceptions of drug dealers. Perpetuity Research & Consultancy International, Leicester

Brown P, Richman H (1993) Communities and neighborhoods: how can existing research inform and shape current urban change initiatives? Background memorandum prepared for the social science research council policy conference on persistent poverty

Brymer RA (1967) Toward a definition and theory of conflict gangs. Paper presented at the annual meeting of the society for the study of social problems, San Francisco, CA

Bullock K, Tilley N (2002) Shootings, gangs and violent incidents in Manchester: developing a crime reduction strategy. Crime reduction research series paper, vol 13, Home Office, London

Bullock K, Clarke RV, Tilley N (eds) (2010) Situational prevention of organised crimes. Taylor & Francis

Burgess RL, Akers RL (1966) A differential association-reinforcement theory of criminal behavior. Social Problems 14(2): 128–147

Butterfield F (1996) In Boston, nothing is something. New York Times, November 21

Campaign (2013) History of advertising No 79: The first drink-drive commercial, Campaignlive.co.uk, 10 Oct. 2013. Accessed 16 Jan 2014

Carlson A (2012). How parents influence deviant behavior among adolescents: an analysis of their family life, their community, and their peers. Perspectives. University of New Hampshire

Caruso R (2011) Crime and sport participation: evidence from Italian regions over the period 1997–2003. The Journal of Socio-Economics, 40(5):455–463

Cayman News Service (2013) Gangs remain key cop issue, Caymannewsservice.com, 25 Jun 2013.

Central Intelligence Agency (2013) The world factbook: Bermuda. The Central Intelligence Agency. Accessed 9 Sept 2013 https://www.cia.gov/library/publications/the-world-factbook/geos/bd.html

Champod C, Lennard C, Margot PA (1993) Alphonse Bertillon and dactyloscopy. Journal of Forensic Identification, 43:604–625

Clarke RV (1997) Situational crime prevention: successful case studies, 2nd edn. Harrow and Heston, New York, pp 1–43

Clarke RV, Weisburd D (1994) Diffusion of crime control benefits: observations on the reverse of displacement. In: Clarke RV (ed) Crime prevention studies, vol 2. Criminal Justice Press, Monsey, pp 165–182

Close Protection World (2010) ARV Officers wanted in Bermuda, closeprotectionworld.com. Available from, http://www.closeprotectionworld.com/police-armed-response-forum/40170-arv-officers-wanted-bermuda.html. Accessed 2 Feb 2014

Coleman R (2003a) Images from a Neoliberal City: the state, surveillance and social control. Critical Criminology: An International Journal, 12(1):21–42

Coleman R (2003b) CCTV surveillance, power and social order: the state of contemporary social control. In: Whyte D, Tombs S (eds) Researching the crimes of the powerful: scrutinising states and corporations. Peter Lang, New York, pp 88–104

Comeau K (2012) 'Building a policy to reduce Bermuda's gang violence.' Good Governance Institute of Bermuda, 19 Jan 2012. Available from http://bdagoodgov.org/?p=121. Accessed 29 Sept 2013

Corbin J (2003) The base: Al-Qaeda and the changing face of global terror. Pocket Books, London, pp 41–53

Cordner G (1998) Community policing: elements and effects. In: Alpert G, Piquero A (eds) Community policing: contemporary reading. Waveland Press, Illinois

Covey HC (2003) Street gangs throughout the world. Charles C. Thomas, Springfield

Covey HC, Menard S, Franzese RJ (1997) Juvenile gangs, 2nd ed. Charles C. Thomas, Springfield

Crabbe T (2000) A sporting chance? Using sport to tackle drug use and crime. Drugs: Education Prevention and Policy, 7(4):381–391

Cragin K (2007) Understanding terrorist ideology, Rand Corporation, Before the Select Committee on Intelligence, United States Senate, 12 June 2007

Criminal Justice Review Team (1992) Report of the criminal justice review board. Criminal justice review team. Available from http://decouto.bm/reports/Tumin-Report-1992-10-02.pdf. Accessed 15 Sept 2013

Curry GD, Decker SH (2003) Confronting gangs: crime and community, 2nd ed. Roxbury, Los Angeles

Curry GD, Ball RA, Decker SH (1996) Estimating the national scope of gang crime from law enforcement data. In: Research in brief. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, Washington. NCJ 161477

Dale A (2009) Conflict could widen as gang step "Outside rules of engagement," Says Pastor,' RoyalGazette.com, 18 Dec 2009. Accessed 3 Dec 2013

Decker SH (2003) Advertising against crime: the potential impact of publicity in crime prevention. Criminology and Public Policy 2:525–530

Decker SH, Curry GD (2003) Suppression without prevention, prevention without suppression. In: Decker SH (ed) Policing gangs and youth violence. Wadsworth/Thompson Learning, Belmont, California, pp 191–213

Decker SH, Van Winkle B (1996) Life in the gang: family, friends, and violence. Cambridge University Press, New York

Decker SH, Weerman FM (eds) (2005) European street gangs and troublesome youth groups. AltaMira Press, Walnut Creek, CA

Delsol R, Shiner M (2006) Regulating stop and search: a challenge for police and community relations in England and Wales. Critical Criminology 14(3):241–263

Department for National Drug Control (2007) Bermuda police service arrest data. Arrest data for the period of 2003–2007. Department for National Drug Control and Ministry of Culture and Social Rehabilitation. Accessed 3 Jan 2014

Department of Defense (US) (2014) 2014 Quadrennial defense review. Department of Defense: http://www.defense.gov/

Department of Statistics (2010) 2010 Census of population and housing, final result. Bermuda. Available from http://unstats.un.org/unsd/demographic/sources/census/2010_phc/bermuda/Bermuda_new.pdf. Accessed 2 Jan 2014

Dickey WJ, Hollenhorst P (1999) Three-strikes laws: five years later. Corrections Managers Quarterly 3(3):1–18

Drake CJM (1998) Terrorist's targeting selection. Palgrave Macmillan

Durkheim E [1893] (1933) The division of labour in society. Trans by George Simpson. The Macmillan Publishing Co, New York. Available from http://www.amazon.com/Division-Labor-Society-Emile-Durkheim/dp/1420948563. Accessed 12 Jan 2014

Weisburd D, Wyckoff LA, Ready J, Eck, JE, Hinckle JC, Gajewski F (2006) Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits. Criminology 44(3) Sept 2006

Ehlers L, Tait S (2009) Finding the right balance: immediate safety versus long-term social change. SA Crime Q 27:23–30

Esbensen FA (2000) Preventing adolescent gang involvement. Youth Gang Series. U.S. Department of Justice, Washington. Office of Juvenile Justice and Delinquency Prevention. Available from http://www.ncjrs.gov/pdffiles1/ojjdp/182210.pdf. Accessed 11 Dec 2013

Esbensen FA, Winfree LT Jr, He N, Taylor TJ (2001) Youth gangs and definitional issues: when is a gang a gang, and why does it matter? Crime Delinquency 47:105–130

Faith R (2014) China's massive tiny land grab continues. Vice.news.com. Vice News, March 12, 2014

Farrington DP (1992) Criminal career research in the United Kingdom. British Journal of Criminology 32:521–536

Fielding N (1995) Community policing. Clarendon Press, Oxford

Foucalt M (1980) Power/knowledge. In: Gordon C (ed). Pantheon Books, NY

Friedman T (2009) No way, no how, not here. The New York Times. 17 Feb 2009. Retrieved 4 Apr 2015

Friendship C, Thornton D (2001) Sexual reconviction for sexual offenders discharged from prison in England and wales. British Journal of Criminology 41:29–39

Fuller B (2010) 'Cayman's gang culture', CompassCayman.com. The observer on sunday, 10 Jan 2010. Available from, http://www.compasscayman.com/observer/2010/01/10/Cayman's-gang-culture/. Accessed 3 Aug 2013

Furedi F (2012) 'Who's afraid of the big bad 'Lone Wolf'?'. Spiked, 22 Feb 2012

Garofalo J, McLeod M (1986) Improving the effectiveness and utilization of neighborhood watch programs. Unpublished report to the National Institute of Justice from the State University of New York at Albany, Hindelang Criminal Justice Research Center

Geason S, Wilson P (1988) Crime prevention theory and practice. In: Wilson P (ed) Missing children. Australian Institute of Criminology

Government of Bermuda (2013) Environmental statistics compendium 2013. A report by the Department of Statistics. Available from http://www.royalgazette.com/assets/pdf/RG1451161030.pdf. Accessed 12 Jan 2014

Grabosky PN (1996) From Politics and practice of situational crime prevention. In: The politics and practice of situational crime prevention: crime prevention studies, vol 5. Ross Homel, pp 25–56

Greene JR (2000) Community policing in America: changing the nature. Structure and function of the police. In: Criminal justice 2000, vol 3: Policies, processes and decisions in the criminal justice system. National Institute of Justice: Washington, pp 299–370

Gurr TR, Grabosky PN, Hula RC (1977) The politics of crime and conflict: a comparative history of four cities. Sage, Beverly Hills

Hagedorn JM, Macon P (1988) People and folks: gangs, crime, and the underclass in a Rustbelt City. Lake View Press, Chicago

Hall T, Gibbons C (2008) Teenager charged in double murder. BDA sun online edition. The Bermuda Sun, 2 Feb 2009. Available from http://bermudasun.bm/Content/NEWS/News/Article/Teenager-charged-in-double-murder/24/270/39055. Accessed 6 Aug 2013

Hamlin J (2001) A non-causal explanation: containment theory. University of Minnesota, Walter C. Reckless', Minnesota

Her Majesty's Inspectorate of Constabulary (2012) Bermuda police service—public document, an inspection commissioned by his excellency. Sir Richard Gozney, KCMG CVO, Governor and Commander-in-Chief and Michael DeSilva, CPM FCMI, Commissioner of Police

Hirschi T (1969) Causes of delinquency. University of California Press, Berkeley and Los Angeles

Holmes J (2015) The two words that explain China's assertive naval strategy. Foreignpolicy.com, 3 June 2015

Howell JC (1998) Youth gangs: an overview. Juvenile justice bulletin. Youth gang series. Office of Juvenile Justice and Delinquency Prevention. U.S. Department of Justice, Washington. Available from http://www.ncjrs.gov/pdffiles/167249.pdf. Accessed Nov 2 2013

Howell JC (2010) Gang prevention: an overview of research and programs. Juvenile justice bulletin. Office of Juvenile Justice and Delinquency Prevention

Hughes G, Edwards A (2005) Crime prevention in context. In: Tilley N (ed) Handbook of crime prevention and community safety. Willan Publishing, Cullompton

Jennings WG (2006) Revisiting prediction models in policing: identifying high-risk offenders. American Journal of Criminal Justice 31(1):35–50

Johnston-Barnes O (2011) Retribution was shooting motive, court told. RoyalGazette.com, 17 June 2011. Available from http://www.royalgazette.com/article/20110617/NEWS02/706179993/0/NEWS Accessed 9 Jan 2014

Jones S (2010a) Four arrested after weekend of violence. BDA sun online edition. The Bermuda Sun, 4 Apr 2010. Available from, http://www.bermudasun.org/Content/FEATURES/Community—Business/Article/Four-arrested-after-weekend-of-violence/60/1315/45564. Accessed 2 Aug 2013

Jones S (2010) Police recruit U.K. gangbuster. BDA sun online edition. The Bermuda Sun, 02 July 2010. Available from http://bermudasun.bm/Content/NEWS/News/Article/Police-recruit-U-K–gangbuster/24/270/46968. Accessed 10 May 2013

Jones S (2011a) UK cops called into crack cold case crimes. BDA sun online edition. The Bermuda Sun, 21 Jan 2011 Available from, http://bermudasun.bm/Content/NEWS/News/Article/UK-cops-called-in-to-crack-cold-case-crimes/24/270/54824. Accessed 12 May 2013

Jones S (2011b) Schoolboys influenced by 'glamorous' gangs. BDA sun online edition. The Bermuda Sun, 20 May 2011. Available from http://bermudasun.bm/Content/NEWS/News/Article/Schoolboys-influenced-by–glamorous–gangs/24/270/52199. Accessed 10 Jan 2013

Jones S (2015) Police treat terrorist Graffiti as 'serious'. RoyalGazette.com. 27 Feb 2015

Jones S, Whittaker J (2009) Violence is driving fans away from football. BDA sun online edition. The Bermuda Sun, 21 Oct 2009. Available from http://bermudasun.bm/Content/NEWS/News/Article/Violence-is-driving-fans-away-from-football/24/270/43190. Accessed 2 Jan 2014

Kelly KD, Caputo T, Jamieson W (2005) Reconsidering sustainability: some implications for community based crime prevention. Crit Soc Policy 25(3):306–324

Kemshall H (2001) Risk assessment and management of known sexual and violent offenders: a review of current issues. Home Office: Police Research Series paper 140

Kemshall H (2002) Risk assessment and management of known sexual and violent offenders: a review of current issues. Scottish Executive Social Research, Crime and Criminal Justice, Edinburgh

Kennedy DM (2011) Don't shoot, one man, a street fellowship and the end of violence in inner-city America. Bloomsbury, New York

Kennedy DM, Piehl AM, Braga AA (1996) Youth violence in Boston: gun markets serious youth offenders, and a use-reduction strategy. Law and Contemporary Problems 59:147–196

Kimery A (2015) UPDATED—AQAP operatives boast Charlie Hebdo's Jihadi attackers, now dead, were their own; more attacks may be planned. Homeland Security Today. 8th Jan 2015. Retrieved 9th Jan 2015

Klein MW (1995) The American street gang. Oxford University Press, New York

Klein MW, Maxson CL (1989) Street gang violence. In: Weiner N, Wolfgang M (eds) Violent crimes, violent criminals. Sage, Thousand Oaks

Klein MW, Maxson CL (2006) Street gang patterns and policies. Oxford University Press, Oxford

Knepper P (2007) Criminology and social policy. Sage, London

Kowalski N (2013) Bermuda's true population: a quarterly economic update by anchor investment management. Available from http://www.anchor.bm/News/RG04112013.pdf. Accessed 12 Jan 2014

LaCourse D (1994) Three strikes is working in Washington. Journal of Interpersonal Violence 9 (3):421–424

Limandri BJ, Sheridan D J (1995) The prediction of intentional interpersonal violence: an introduction. In: Campbell J (ed) Assessing dangerousness: violence by sexual offenders, batterers, and child abusers. Interpersonal violence: the practice series: Sage: 1–19

Linton DL (1955) The problem of tors. The Geographical Journal 121:470–87. Available from http://ppg.sagepub.com/content/18/4/559.extract. Accessed 10 Jan 2014

Loeber R, Farrington DP, Stouthamer-Loeber M, van Kammen WB (1998) Antisocial behaviour and mental health: explanatory factors in childhood and adolescence. Eribaum, Mahwah

Loveday B (1994) Government strategies for community crime prevention programmes in England and Wales: a study in failure? International Journal of the Sociology of Law 22 Part 3

Manning P (1988) Community policing as a drama of control. In: Greene J, Mastrofski S (eds) Community policing: rhetoric or reality?. Praeger, New York

Manning P (1993) Community-based policing. In: Dunham R, Alpert G (eds) Critical issues in policing. Waveland Press, Prospect Heights, IL

Maslow AH (1943) A theory of human motivation. Psychol Rev 50:370–396

Mastrofski S (1998) Community policing and police organization structure. In: Brodeur JP (ed) How to recognize good policing: problems and issues. Sage and Police Executive Research Forum, Thousand Oaks

Meares T, Kahan D (1998) Law and (Norms of) order in the inner city. 32 Law Soc Rev 80:5–37

Melathe A (2014) Meet the 17-year-old who blew the lid off racial profiling with his iPod. UpWorthy.com. Available from, http://www.upworthy.com/meet-the-17-year-old-who-blew-the-lid-off-racial-profiling-with-his-ipod?c=reccon1. Accessed 1 Feb 2014

Miethe TD (1991) Citizen based crime control activity and victimization risks: an examination of displacement and free-rider effects. Criminology 29:419–440

Miller J, Bland N, Quinton P (2000) The impact of stops and searches on crime and the community. Police Research Series Paper 127. Home Office, London

Mohan G, Stokke K (2000) Participatory development and empowerment. Third World Q 21(2): 266–280

Moore M (1992) Problem-solving and community policing. In: Tonry M, Morris N 15 (eds) Modern policing (Crime and justice—a review of research vol 15). University of Chicago Press, Chicago

Morrison A (2015) After Paris attacks, middle class jihadists debunking myth that all Islamic extremists are poor and disenfranchised. International Business Times. 18 Nov 2015

Muncie J (1999) Deconstructing criminology. Criminal Justice Matters 34:4–5

Musson NM (1979) Mind the onion seed: black roots, Bermuda. Parthenon Press, Nashville

NASRO (2012) To protect and educate: the school resource officer and the prevention of violence in schools. National Association of School Resource Officers

National Gang Center (2011) National youth gang survey analysis. Available from http://www.nationalgangcenter.gov/Survey-Analysis. Accessed 2 Jan 2014

Newman O (1972) Defensible space. Macmillan, New York

Nichols G (1997) A consideration of why active participation in sport and leisure might reduce criminal behaviour. Sport Educ Soc, vol 2(2)

Nichols G, Crow I (2004) Measuring the impact of crime reduction interventions involving sports activities for young people. The Howard Journal 43(3):267–283

Nichols G, Taylor P (1996) West Yorkshire sports counselling: final evaluation. West Yorkshire Sports Counselling Association, West Yorkshire, England

Palmer A (2008) ‘Crime stats’, Bermuda.org.uk. Available from http://www.bermuda.org.uk/crime_stats.htm. Accessed 6 Sept 2013

Parliamentary Joint Select Committee (2011) Joint select on the causes of violent crime and gun violence in Bermuda: a parliamentary joint select committee publication under part IV of the Parliamentary Act 1957, July 2011. Available from http://www.parliament.bm/uploadedFiles/Content/Home/Report%20on%20Violent%20Crime%20and%20Gun%20Violence%20in%20Bermuda.pdf. Accessed 11 Nov 2012

Parnaby PF (2006) Crime prevention through environmental design: discourses of risk, social control, and a neo-liberal context. Canadian Journal of Criminology and Criminal Justice, 48(1):1–30

Peak K, Glensor R (1999) Community policing and problem solving: strategies and practices, 2nd edn. Prentice Hall, New Jersey

Pearman MI (2011) Expert lifts the lid on gangs. Bermuda sun online edition, The Bermuda Sun, 25 Nov 2011. Available from http://bermudasun.bm/Content/NEWS/News/Article/Expert-lifts-the-lid-on-gangs/24/270/55457. Accessed 20 Jan 2014

Pedahzur A (2004) Toward an Analytical Model of Suicide Terrorism—A Comment, Terrorism and Political Violence, 16(4):842–843

Pharaoh R (2005) An unknown quantity: kidnapping for ransom in South Africa. Available from http://www.iss.co.za/pubs/crimeQ/No.14/pharaoh.pdf. Accessed 29 Nov 2013

Podolefsky A (1984) Rejecting crime prevention programs: the dynamics of program implementation in a high need community. Human Organization 44:33–40

Poole D (1997) Building community capacity to promote social and public health: challenges for universities. Health and Social Work 22:163–170

Poyner B, Webb B (1987) Successful Crime Prevention: Case Studies. London: Tavistock Institute of Human Relations

Raco M (2007) Securing sustainable communities: citizenship, safety and sustainability in the new urban planning. European Urban and Regional Studies 14(4):305–320

Reckless WC (1973) The crime problem, 5th edn. Goodyear Publishing Company, Pacific Palisades

Reich W (1998) Origins of terrorism: psychologies, ideologies, theologies, states of mind. Woodrow Wilson Center Press, Washington

Roberts E (2009) Unsolved murder cases could be cracked, detectives hope. RoyalGazette.com, 7 May 2009. Available from http://www.royalgazette.com/article/20090507/NEWS/305079982. Accessed 12 Dec 2013

Robins S (2010) Cayman islands calls in UK police as crime threatens image. JamaicaObserver.com, The Jamaica Observer, 21 May 2010. Available from, http://www.jamaicaobserver.com/news/Cayman-Islands-calls-in-UK-police-as-crime-threatens-image_7630605. Accessed 3 Aug 2013

Rosenbaum D (1998) The changing role of the police: assessing the current transition to community policing. In: Brodeur JP (ed) How to Recognize Good Policing: Problems and Issues. Sage and Police Executive Research Forum, Thousand Oaks

Rothkopf D, Casey C (2014) Impacts of climate change, resource scarcity and foreign policy. worldwildlife.org, World Wildlife Magazine, Winter 2014

Ryan J (2009) Gangs blamed for 80 Percent of U.S. crimes, abcnews.go.com, ABC News, 30 Jan 2009. Available from http://abcnews.go.com/TheLaw/FedCrimes/story?id=6773423&page=1. Accessed 3 Aug 2013

Sanchez-Jankowski M (1991) Islands in the street: gangs in American urban society. University of California Press, Berkeley

Sanders WB (1994) Gangbangs and drive-bys: grounded culture and juvenile gang violence. Aldine De Gruyter, New York

Scherdin MJ (1986) The Halo effect: psychological deterrence of electronic security systems. Information Technology and Libraries 5:232–235

Schifrin N (25 November 2009) Mumbai terror attacks: 7 Pakistanis charged—action comes a year after India's worst terrorist attacks: 164 Die'. ABC News

Schmid AP (2012) The revised academic consensus definition of terrorism. Perspectives on Terrorism 6(2)

Schoenberg A (1983) Theory of harmony. University of California Press

Scott M (2011) Offenders to get electronic bracelets. BDA sun online edition, 18 Oct 2011. Available from http://www.bdasun.bm/Content/NEWS/News/Article/Offenders-to-get-electronic-bracelets/24/270/54738. Accessed 11 June 2013

Seepersad R, Bissessar M (2013) Gangs in the Caribbean. Cambridge Scholars Publishing, Newcastle upon Tyne

Sherman L (1990) Police crackdowns: initial and residual deterrence. In: Tonry M, Morris N (eds) Crime and justice: a review of research, vol 12. University of Chicago Press, Chicago

Sherman L, Gottfredson D, MacKenzie D, Eck J, Reuter P, Bushway S (1997) Preventing crime, what works, what doesn't, what's promising. U.S. Department of Justice, Washington, Chapter 8

Skinner C (2013) U.S. crime rate rising, but fewer Americans believe it: gallup poll. Reuters, Malone S, Burgdorfer B (eds) Thomson Reuters, 31 October 2013. Available from http://www.reuters.com/article/2013/10/31/us-usa-poll-crime-idUSBRE99U11Z20131031. Accessed 19 Jan 2013

Skogan WG (1986) Fear of crime and neighborhood change In: Reiss Jr AJ, Tonry M (eds) Communities and crime. Chicago: University of Chicago Press

Smith C (2013) Beyond rugby Bermuda is the model programme. RoyalGazette.com, 5 July 2013. Available from http://www.royalgazette.com/article/20130705/COLUMN13/707059981. Accessed 24 Jan 2014

Smith MJ, Clarke RV (2012) Situational crime prevention: classifying techniques using 'Good enough' theory. The Oxford Handbook of Crime Prevention, 291

Stevenson C (2014) Man charged with murder, RoyalGazette.com, 20 Jan 2014. Available from http://www.royalgazette.com/article/20140120/NEWS/140129972. Accessed 20 Jan 2014

Stouthamer-Loeber M, Loeber R, Wei E, Farrington DP, Wikström P-OH (2002) Risk and promotive effects in the explanation of persistent serious delinquency in boys. Journal of Consulting and Clinical Psychology 70:111–123

Strangeways S (2010) Bermuda's per capita murder rate was more than five times London's rate in 2009. RoyalGazette.com, 9 Jan 2010. Available from http://www.royalgazette.com/article/20100109/NEWS/301099993. Accessed 13 Sept 2013

Strangeways S (2011a) Gun murder in 2003 was a 'Catalyst' for today's killings. RoyalGazette.com, 26 Aug 2011. Available from http://www.royalgazette.com/article/20110826/NEWS10/708269940/gun-murder-in-2003-was-a-145-catalyst-146-for-today-146-s%26utm_source%3Dnewsletter20110826%26utm_medium%3Demail%26utm_content%3Darticle_title%26utm_campaign%3Dnewsletter. Accessed 9 Dec 2013

Strangeways S (2011b) Motive for murder that sparked cycle of shootings is still a mystery. RoyalGazette.com, 29 Aug 2011. Available from http://www.royalgazette.com/article/20110829/NEWS10/708299940. Accessed 23 Aug 2013

Strangeways S (2011c) Cann case stalls over lack of evidence. RoyalGazette.com, 6 Sept 2011. Available from http://www.royalgazette.com/article/20110906/NEWS10/709069921. Accessed 5 May 2013

Strangeways S (2011d) Murder rate is double the world average. RoyalGazette.com, 21 Nov 2011. Available from http://www.royalgazette.com/article/20111121/NEWS03/711219957. Accessed 5 May 2013

Strangeways S (2011e) Public can help crack unsolved murders', RoyalGazette.com 29 Aug 2011. Available from http://www.royalgazette.com/article/20110829/NEWS10/708299938/-1&source=RSS. Accessed 12 Aug 2013

Strangeways S (2013) Operation ceasefire launches next month. RoyalGazette.com, 29 Apr 2013. Available from http://www.royalgazette.com/article/20130429/NEWS03/704259885. Accessed 1 Sept 2013

Sullivan JP, Elkus A (2009) Urban siege in South Asia. Open security. www.opendemocracy.net. 9 Nov 2009. Accessed 21 Apr 2015

Sumner WG (1906) Folkways. Ginn, Boston

Swan Q (2009) Black power and the struggle for decolonization in Bermuda. Palgrave Macmillan, New York

Thacher D (2001) Conflicting values in community policing. Law Soc Rev 35(4). Available from http://sitemaker.umich.edu/dthacher/files/Conflicting%20Values%20in%20CoP.pdf. Accessed 2 Dec 2013

Thacher D, Rein M (2004) Managing value conflict in public policy. Governance 17(4):457–486. Available from http://onlinelibrary.wiley.com/doi/10.1111/j.0952-1895.2004.00254.x/full. Accessed 12 Jan 2014

The Bermuda Sun (2007) Getting away with murder. BDA sun online edition, 28 Dec 2007. Available from, http://www.bermudasun.bm/Content/NEWS/News/Article/-Getting-away-with-murder-/24/270/36207. Accessed 3 Aug 2013

The Bermuda Sun (2010) Gangs can be defeated. BDA sun online edition, 26 Mar 2010. Available from http://bermudasun.bm/Content/NEWS/News/Article/-Gangs-can-be-defeated-/24/270/45454. Accessed 2 Aug 2013

The Royal Gazette (2009) Somewhere along the line our methods are failing. RoyalGazette.com, 28 Dec 2009 accessed online

The Royal Gazette (2011a) Case eight: Colford Ferguson. RoyalGazette.com, 18 Aug 2011. Available from http://www.royalgazette.com/article/20111018/NEWS03/710179943. Accessed 3 Aug. 2013

The Royal Gazette (2011b) Crime stoppers facts and figures. RoyalGazette.com, 6 Sept 2011. Available from http://www.royalgazette.com/article/20110906/NEWS10/709069911&source=RSS. Accessed 3 Aug 2013

The Washington Post (2006) Gang violence jolts formerly quiet Bermuda; tourist getaway grapples with string of shootings. HighBeam research, The Washington Post, 6 Aug 2006. Available from http://www.highbeam.com/doc/1P2-139686.html [Accessed, 3 Aug. 2013]

Thornberry TP, Huizinga D, Loeber R (2004) The causes and correlates studies: findings and policy implications. Journal of the Office of Juvenile Justice Delinquency Prev 9:3–19. Reprinted in Bernard TJ (ed) (2006) Serious delinquency: an anthology, pp 39–52. Roxbury, Los Angeles

Thrasher FM (1927; abridged ed 1963) The gang: a study of 1313 gangs In Chicago. University of Chicago Press, Chicago

Tita G, Riley KJ, Greenwood P (2003) From Boston to Boyle heights: the process and prospects of a “Pulling Levers” strategy in a Los Angeles Barrio. In: Decker S (ed) Policing gangs and youth violence. Wadsworth, Thousand Oaks, pp 274–277

United Nations (2010) Manual on victimization surveys: a report by the United Nations office on drugs and crime and United Nations Economic Commission for Europe

United Nations (2011) Global study on murder: trends/contexts/data: a report by the United Nations office on drugs and crime

United Nations (2012a) Human development and the shift to better citizen security. Caribbean human development report 2012

United Nations (2012b) Murder statistics, 2012: a report by the United Nations office on drugs and crime

U.S. Congress, Congressional Research Service (2013) The federal prison population buildup: overview, policy changes, issues, and options. James N. Cong Rept 7-5700. Washington, D.C.: Congressional Research Service, 2013. Print

U.S. Sentencing Commission (2011) Report to congress: mandatory minimum penalties in the federal criminal justice system, Washington, DC, October 2011, p 63. Available from http://www.ussc.gov/Legislative_and_Public_Affairs/Congressional_Testimony_and_Reports/Mandatory_Minimum_Penalties/20111031_RtC_Mandatory_Minimum.cfm. Accessed 19 Jan 2014

Vigil JD (2002) A rainbow of gangs: street cultures in the mega-city. University of Texas Press, Austin

Waller I, Weiler D (1984) Crime prevention through social development: an overview with sources. Canadian Council on Social Development, Ottawa

Wells P (2004) The worst of Bermuda awards 2004. A limey in Bermuda. Available from, http://www.limeyinbermuda.com/2004/07/the_worst_of_be.html. Accessed 2 Feb 2014

Wells HG (2008) BERMUDA: paradise lost and rise of a dictator. Bermudaparadiselost.blogspot.co.uk. Available from, http://bermudaparadiselost.blogspot.co.uk. Accessed 2 Sept 2013

Whittaker J (2013) Clampdown hard on violent crime, expert warns. CompassCayman.com, Compass Cayman, 7 Oct 2013. Available from http://www.compasscayman.com/caycompass/2013/10/07/Clampdown-hard-on-violent-crime,-expert-warns/. Accessed 3 Nov 2013

Wilson C (2012a) Police hail somerset dispersal success. RoyalGazette.com, 13 June 2012. Available from http://www.royalgazette.com/article/20120613/NEWS03/706139913/1001. Accessed 18 May 2013

Wilson C (2012b) ‘Inter-agency’ gang task force members back from Boston tour. RoyalGazette.com, 12 Oct 2012. Available from http://royalgazette.bm/article/20121012/NEWS03/710129912. Accessed 18 May 2013

Wilson C (2013a) More than $1 m seized under the proceed of crime act. RoyalGazette.com, 27 Feb 2013. Available from http://rg.bm/article/20130227/NEWS03/702279940. Accessed 17 May 2013

Wilson C (2013b) Public safety minister announces cash-for-guns scheme. RoyalGazette.com, 12 Apr 2013. Available from http://www.royalgazette.com/article/20130412/NEWS/704129909. Accessed 17 May 2013

Wilson C (2013c) Increased policing patrols for halloween. RoyalGazette.com, 29 Oct 2013. Available from http://www.royalgazette.com/article/20131029/NEWS/131029662. Accessed 3 Dec 2013

Wilson C (2013d) DeSilva: my gun crime frustration. RoyalGazette.com, 18 Sept. 2013. Available from http://www.royalgazette.com/article/20130918/NEWS/130919710. Accessed 7 Sep 2014

Wilson JQ, Kelling GL (1982) Broken windows: the police and neighborhood safety. Atlantic Monthly 249:29–38

Winship C, Berrien J (1999) Boston cops and black churches. Public Interest 136:52–68

Witkin G (1997) Sixteen silver bullets: smart ideas to fix the world. U.S. News and World Report, 29 December 1997, p 67, referenced from http://www.usnews.com/usnews/culture/articles/971229/archive_008861.htm. Accessed 10 Jan 2014

Wyrick PA (2006) Gang prevention: how to make the “Front End” of your anti-gang effort work. US Attorneys’ Bulletin 54:52–60

YouTube (2014) CCTV court street shooting. YouTube.com. Available from http://www.youtube.com/watch?v=EIGJX5-3RIc. Accessed 2

Scanning the Consequences of Demographic Change for the Emerging Security Landscape

Christian Leuprecht

Abstract This chapter peruses the causes, consequences and implications of changes in the supply and demand side of consequences of demographic change as a non-traditional transnational challenge in the emerging security problem space. Demography is the study of population structure and change as a result of interaction effects among fertility, mortality and immigration. Political demography is the study of how change in the size, distribution, and composition of population affects both politics and government. It examines communal relations, political behaviour and social institutions as a process of change in demographic trends. This chapter in particular surveys distributive effects of resources and political power as a result of changing urban and rural, religious, regional, ethnic, elite, and cohort population subgroups, and their impact on domestic, regional and global security environments.

Keywords Political demography · Fertility · Mortality · Immigration · Security · Defence · Intervention · Recruitment · Retention · Allies

1 Introduction

Demographic cleavages are to the 21st century what class divisions were to the 19th century. Rarely can social scientists claim to be observing genuinely unprecedented phenomena. The world's contemporary demographic developments, however, are without historical precedent: women are consistently having fewer or no children than at any previous time in history, never have there been as many people on the planet, has the world's population expanded as rapidly in as short a period of time

Parts of this chapter are a revision of the author's entry in the The Encyclopedia of Public Administration and Public Policy. 3rd Ed. Bearfield D & Dubnick M, Eds. New York: Taylor and Francis 2015; Vol 4, pp. 2983–2992.

C. Leuprecht (✉)
Royal Military College of Canada, Kingston, Canada
e-mail: christian.leuprecht@rmc.ca

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_7

(5 billion people over the course of a century), have people lived longer and populations grown as old, have there been more people of working age, and have as many children lived in the developing world. For the first time in history, more people now live in cities than on the land. Is it sheer coincidence that the mature industrialized democracies have aging population structures and no longer go to war with one another while states with young populations that are growing rapidly tend to be disproportionately prone to violent conflict?

Between 2008 and 2010, Gallup conducted a rolling survey of 401,490 people across 146 countries. It found that 14 % of the world's population—some 630 million people—would like to migrate to another country if they could. People across sub-Saharan Africa (33 %), North Africa (23 %) and the Middle East, and Latin America (23 %), had the greatest urge to move permanently. The United States as the destination of choice (23 %) is followed by Canada and the United Kingdom (7 % each). "Just as no credible political scientist can afford to ignore the role of economic incentives, institutions, or culture, [...] political scientists cannot afford to ignore demography in seeking to understand patterns of political identities, conflict, and change (Kaufmann and Duffy Toft 2011: 3)." The next four decades will present unprecedented changes in long-term demographic trends, including the shrinkage of Europe's labour force, the extreme aging of the advanced industrial societies, a global shift from mainly rural to mainly urban habitation, and a substantial turn in global economic growth toward the developing world (where 9 out of every 10 of the world's children under 15 now live).

The first section traces demography as a major process of change in contemporary societies. The second section surveys the causes of population aging. The third section discusses the consequences of the demographic economy from the perspective of national defence. The fourth section discusses the supply and the demand side of consequences of demographic change for security. The demand side is concerned with the way demographic change affects stability: local, domestic, regional, international and transnational. Contrast this with the supply side, where there are fewer countries and reduced capability to respond to greater demand for international interventions. The conclusion ponders broader implications of these observations for conflict and cooperation.

2 Scanning the Demographic Horizon

Demographic trends allow us to anticipate future developments in size and distribution of population groups. As such, demography is a harbinger of challenge and opportunity, a multiplier of conflict and progress, and a resource for power and prosperity (Winter and Teltelbaum 2013; Dabbs Sciubba 2011a, b). In fact, fertility, mortality and migration are the only set of variables in the social sciences that can be projected forward over the medium term with a high degree of accuracy: the population that will be growing old over the coming decades has already been born and we also know the average number of children to which a woman in a given location is likely to give birth. Until fairly recently, high birth rates had kept populations fairly young. Due to war and epidemics, such as the plague, few people ended up growing old (Anderson 1996). Innovations in public health and food security changed that. The result was a decline in death rates. Birth rates would initially remain high before eventually leveling off. That change in birth and death rates, and the delta between them, is largely responsible for the phenomenon depicted in Fig. 1, known as the demographic transition.

Yet, the demographic transitions set in at different times in different countries and among different population groups. As a result, different countries and population groups find themselves at different stages along the demographic transition, which explains why some countries are aging rapidly while others are bulging with youth. Throughout history, the ebb and flow of population—through natural growth, epidemic diseases, and migration—has been linked to the rise and fall of empires, to conquests and revolutions, rebellion, civil war, and the rise and collapse of entire societies and civilizations (Goldstone 1991; Diamond 1997; Leahy et al. 2007; Duffy Toft 2003). Periods when populations were stable in size also tended to be politically quiet. By contrast, when populations grew rapidly, such as the century from 1550 to 1650, or from 1730 to 1850, political dislocation followed. Real wages fell and peasants faced shortages of land; social mobility and competition for elite positions increased as more surviving sons and daughters meant that simple inheritance no longer provided for stable succession; and state and urban administrations were stressed by the need to keep food supplies flowing and to enforce order among rapidly growing populations.

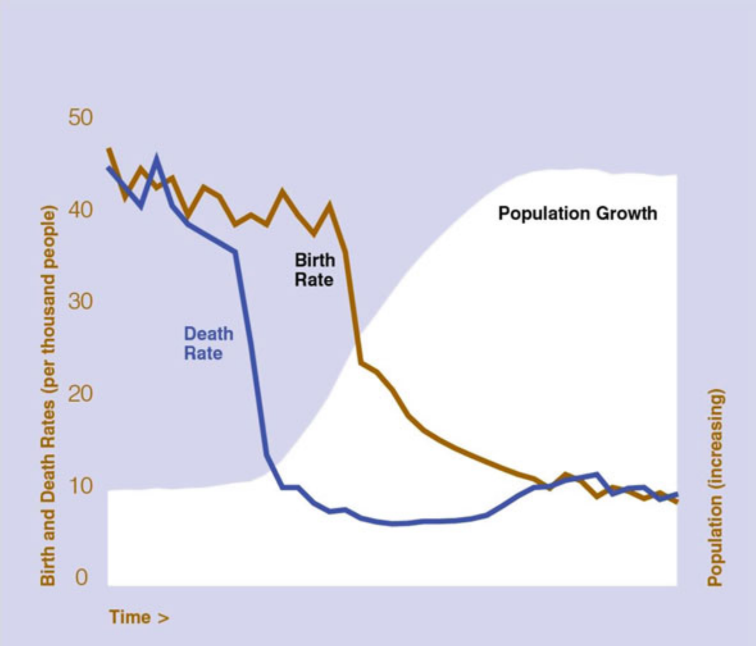


Fig. 1 The demographic transition. *Source* Population Action International, p. 17

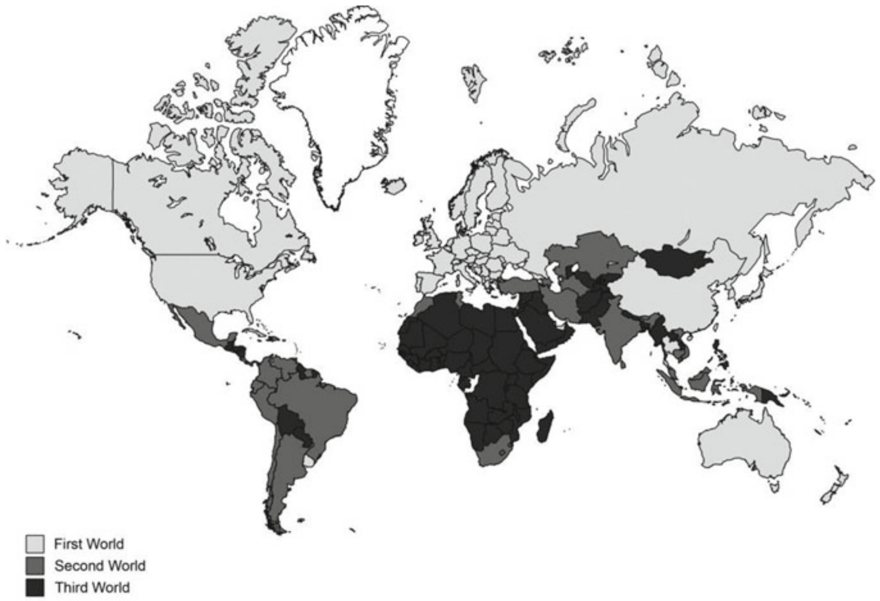


Fig. 2 The three worlds emerging from socio-demographic differentiation. *Source* Angenendt and Apt (2010, p. 8)

On a global scale, Angenendt and Apt (2010) observe demographic differentiation as depicted in Fig. 2: a "first" world that consists of industrialized countries whose populations tend to be affluent, aging, and some in demographic decline; a "second" world that consists of economically dynamic emerging countries where population growth and urbanization is relatively balanced: and a "third" world that consists of poor countries with youthful populations that are growing and urbanizing rapidly.

This socio-demographic partition of the world gives rise to many challenges. Population aging and decline is bound to have economic and political ramifications for developed industrial states. Persistent immigration to these countries offers them prospects for continued growth and affluence while harboring the potential of putting social cohesion and domestic stability at risk. Urbanization is slated to continue apace in many developing countries whose populations are transitioning demographically (United Nations 2014). However, inadequate infrastructure, institutions and financial means, especially in medium-sized cities, which may give rise to domestic tensions. The Least Developed Countries (LDCs) are usually also the least transitioned demographically. Propitious economic and political conditions may yield eventually a "demographic dividend" for their large and rapidly growing cohort of children and youth countries. In the nearer term, however, poverty, hopelessness and poor governance is likely to undermine their economic and social integration. As the potential for conflict rises, so does the incentive to emigrate.

Since democracy has as its foundation the principle of majority rule, states adopting democratic forms of government will find themselves keenly interested in the proportions of the politically active groups that inhabit their territories (Leuprecht 2010a, b, 2011). Population structures within a given country, however, can be heterogeneous: Aboriginal groups tend to have young population structures, as do some religious groups, such as orthodox Jews. These differences can exacerbate conflict, especially as population structures diverge; concomitantly, they can moderate conflict and hasten democratic consolidation as population structures among groups in conflict start to converge (Leuprecht 2012; Kaufmann 2011; Frey 2011). Shifts in population composition can affect who wins and loses political battles, lead to the realignment of political party systems, or fuel violent conflict in fragile and transitional states (Goldstone 2002; Friedman 2014). Demographic factors influence geopolitics, fiscal politics, ethnic and religious conflicts, and voting patterns, all of which have implications for the provision and consumption of collective security.

3 Population Aging

With the exception of the United States, all NATO members have been beset by population aging. The scope of this aging process is remarkable. By 2050, at least 20 % of the population in allied countries will be over 65. This demographic development is historically without precedent; we know neither what to expect from a state with over one-third of its population over 60, nor how its economic growth and finances will be affected (Bloom and Canning 2011). Most of the world's affluent countries—in Europe, East Asia (Japan, South Korea, Taiwan, Singapore), and North America—have completed their demographic transition and have stable or very slow-growing populations. For a state to sustain its population (assuming zero net immigration), fertility levels must exceed about 2.1 children per woman. Today the United States is the only liberal democracy that comes close to meeting this requirement. Most other liberal democracies fell below this threshold some time ago. A growing number of states, including Germany and many in Eastern Europe, have seen their Total Fertility Rate fall well below 2.0 children per woman; so, they are forecast to decline in population in the foreseeable future (Table 1).

Never before has humanity witnessed such dramatic, widespread aging among the world's most industrialized and powerful military allies. Two long-term demographic trends coincide to produce population aging: decreasing fertility rates and increasing life expectancy. These developments have only a moderate effect on the pecking order among the world's three most populous countries. Yet, the impact on "the rise and fall" of other "great powers" (measured by population size), as Table 2 shows, is marked: by 2050 Nigeria is projected to displace the United States as the third most populous country in the world.

Table 1 Countries projected to have declining populations, by period of the onset of decline, 1981–2045

Already declining	Onset of decline: 2009–2029	Onset of decline: 2030–2050
Hungary (1981)	Italy (2010)	Azerbaijan (2030)
Bulgaria (1986)	Slovakia (2011)	Denmark (2031)
Estonia (1990)	Bosnia and Herzegovina (2011)	Belgium (2031)
Georgia (1990)	Greece (2014)	Thailand (2033)
Latvia (1990)	Serbia (2014)	North Korea (2035)
Armenia (1991)	Serbia (2014)	Singapore (2035)
Romania (1991)	Portugal (2016)	Netherlands (2037)
Lithuania (1992)	Cuba (2018)	Switzerland (2040)
Ukraine (1992)	Macedonia (2018)	UK (2044)
Moldova (1993)	Spain (2019)	Puerto Rico (2044)
Belarus (1994)	Taiwan (2019)	Kazakhstan (2045)
Russian Federation (1994)	South Korea (2020)	
Czech Republic (1995)	Austria (2024)	
Poland (1997)	Finland (2027)	
Germany (2006)	China (2029)	
Japan (2008)		
Croatia (2008)		
Slovenia (2008)		

Source Adapted from Jackson and Howe; excludes countries with populations less than 1 million

Table 2 Largest countries ranked by population size, 1950, 2005, and 2050

Ranking	1950	2005	2050
1	China	China	India
2	India	India	China
3	United States	United States	Nigeria
4	Russian Federation	Indonesia	United States
5	Japan	Brazil	Indonesia
6	Indonesia	Pakistan	Pakistan
7	Germany	Nigeria	Brazil
8	Brazil	Bangladesh	Bangladesh
9	UK	Russian Federation	Ethiopia
10	Italy	Japan	Philippines
11	Bangladesh	Mexico	Mexico
12	France	Philippines	Congo, DR
		(15) Germany	(16) Japan
		(21) France	(23) France
		(22) UK	(24) UK
		(23) Italy	(25) Germany

Source Department of Economic and Social Affairs, Tables S.3 and S.4, pp. 20–21

4 The Demographic Economy of National Defence

An unprecedented 70 % of people in the developed world are between 15 and 64 years of age. Never before has that proportion been as high—and it is only expected to decline henceforth. This has important implications for not only for consumption, productivity, tax revenue, and fiscal expenditures but, as I explain elsewhere, for military recruitment, retention, personnel costs, the allocation of labour and capital expenditures, force structure, and posture (Jackson and Howe 2011; Janowicz 1960). The costs created by the NATO allies' and great powers' aging populations are bound to constrain spending on economic development and national defence. Population aging causes military-personnel costs to rise. As demographic growth slows but economies continue to grow, the labour market tightens. Concomitantly, the nature of modern military organizations—as Morris Janowicz observed four decades ago—is less and less "an organization set apart" for a uniquely specific purpose, but is instead increasingly approximating any other private- or public-sector organization (European Defence Agency 2006). As a result, it competes for the same highly skilled and educated labour. The combination of a tightening labour market and growing competition of a small pool of highly qualified labour causes salaries to grow exponentially (Moskos 1977).

As population aging stresses the dependency ratio between the old and the young, the provision of international security is partially a function of pension systems. Aging populations and shrinking workforces are forcing NATO-member countries to spend more of their defence budgets on personnel costs and pensions to the detriment of research, development, and procurement of sophisticated technology. In the United States, for instance, about 50 cents of every dollar spent on defence goes to compensation, an amount that, *certeris paribus*, is slated to rise to 70 % before 2030; pension payments amount to over $50 billion a year, health care costs to another $50 billion (of a total US defence budget of about $735 billion in 2014). As military organization continues its shift from an institutional to an occupational format that is driven by self-interest and a free market, these liabilities are projected to rise (Williams 2007). To ensure an all-volunteer force remains an attractive and competitive employer of choice in a tightening labor market, it needs to overhaul compensation systems, increase pay and benefits, and modernize pension plans (Williams 2004; Moskos et al. 1999). Pensions, then, are a liability insofar as they are ongoing and growing obligations that add little value to defence capabilities per se, but an asset in attracting and retaining highly qualified personnel in a tight labour market where secure pensions are increasingly scarce. The substitution effect of capital—manifest in advanced technology—for labor is premised on highly motivated, qualified, trained and skilled operators to contest the fourth- and fifth-generation warfare (Culhane 2001). In opting for quality over quantity, mandatory military service is jettisoned for a professional all-volunteer force. Yet, savings generated through reductions in personnel risk being reallocated to attract and retain highly qualified personnel. Moreover, the cost of intervention is disproportionately borne by those few who commit to military service.

The distributive effects pension obligations have within public and defence budgets stand to be mitigated or exacerbated by the way pension obligations are funded. Funded pension systems, such as those found throughout the Anglosphere—nuances due to demographic differences such as the US baby boom notwithstanding—redistribute income through the purchase of assets by workers and the sale of assets by retirees. They encourage workers to save, thereby increasing capital, productivity and GDP growth (OECD 2011).[31] By contrast, countries such as China, France, Germany, and Russia tend to pay pension obligations out of general revenue (i.e., current contributions, instead of being invested to grow, pay for current liabilities—a system commonly known as "pay as you go"). Ergo, every Euro spent on retirement benefits is one Euro less to spend on other services, let alone weapons, research, or personnel. The United States, the United Kingdom, and Canada, by contrast, use funded pensions to augment social security. Pay-as-you-go systems redistribute revenue from the working-age population to pensioners through taxes. When the benefits paid replace a high proportion of average earnings, they also create a disincentive to save and work past the normal retirement age, both of which depress GDP. In light of population aging, pay-as-you-go systems are fiscally unsustainable because they have to be paid for either through tax increases by the working-age population or through issuance of government debt (thus crowding out defence spending). Yet, many pay-as-you-go countries already register some of the highest marginal tax rates in the world. This is problematic insofar as high payroll taxes are a drag on a workforce's competitiveness. Pay-as-you-go is a vicious circle: As countries raise taxes to pay for pay-as-you-go, their workers become increasingly uncompetitive, thus further undermining the ability to pay for the pay-as-you-go system.

At the same time, the Anglosphere is aging less rapidly than other countries, owing largely to higher fertility rates and immigration. As a result, the pressures of elderly care over defence spending remain favourable, and the increased substitution effect of labour for capital in defence budgets is bound to be smaller. Table 3 is notable for stagnating or declining populations of prime working age due to aging outpacing growth even in countries with high rates of immigration, such as France, Spain, and Switzerland.

While their labour force faces an unprecedented decline, the proportion of their population over 60 years of age will rise by 50 % on average. As Europe, Japan, and South Korea lose one quarter to one-third of their prime labour force by 2050, the dependency gap widens. A growing dependency ratio aggravates the situation further by depressing GDP growth as people work less, exercise their exit option in favour of lower-tax jurisdictions, migrate to the underground economy, opt not to work at all, and, squeezed by high taxes, opt for fewer children.

Owing to comparatively low social security promises, the Anglosphere tends to be less affected by social aging than other allied countries. Americans, for instance, have the highest prediction of when they expect to retire (67.2) and (by far) the lowest expectations regarding governmental support of their retirement (Friedman 2005). Conversely, countries with some of the greatest expenditure burden on aging populations are making matters worse by encouraging early retirement to ease their

Table 3 Aging and labour force change across select countries, 2009–2050, ranked in reverse order of changes in prime working age population

	% Change in:		
	Total population	Population 15–60	Population 60+
Bulgaria	−29	−46	13
Belarus	−24	−42	46
Ukraine	−23	−40	21
Japan	−20	−37	19
Romania	−19	−38	50
Poland	−16	−38	70
Russia	−18	−36	47
S. Korea	−9	−36	146
Germany	−14	−32	32
Hungary	−11	−26	33
Portugal	−6	−26	54
EUROPE	−6	−24	47
Italy	−5	−24	41
Greece	−2	−23	54
Czech Republic	−1	−23	57
Austria	2	−18	59
China	5	−17	175
Spain	14	−13	93
Finland	2	−10	36
Netherlands	5	−9	53
Belgium	8	−7	52
Denmark	1	−6	29
France	9	−6	56
Switzerland	13	−4	56
Sweden	14	4	40
United Kingdom	18	7	51
Canada	32	9	116
United States	28	15	97
Ireland	39	17	164

Source OCED (2011)

unemployment burden while shying away from reducing old-age benefits. The opportunity cost of stressed pension schemes and social services is less money for more sustainable investments in technology to spur gains in productivity. Suboptimal use of productive labour also risks exacerbating social conflict over pensions, migration, and labour/employer relations (Kaufman 2012; Vanhuysee and Goerres 2012; Davidson 2012).

The Anglosphere thus has a greater potential to spend more on defence than some other allies as public policy spending becomes increasing contingent on population aging. This hypothesis is difficult to measure in the short term as either cuts to defence spending, cuts to authorized troop strength, or both, and, consequently, per capita military spending and active soldiers are omnipresent across NATO-member countries, the United States first and foremost among them. Still, the United States' defence budget's expenditure burden within NATO is on the rise: from an apex of almost 77 % in 1952, it bottomed out near parity at 55 % in 1999 (Larrabee et al. 2012). Yet, the spread in transatlantic expenditure bifurcation among NATO member countries has been widening ever since (Leuprecht 2014). Adjusted for constant prices and exchange rates, the current US contribution to NATO could be argued to be approaching 75 %. Over the same period, the authorized active strength of Canada's, Australia's and New Zealand's armed forces has remained remarkably stable while that of the US and United Kingdom has been on the wane. Yet, total military spending cannot be readily parlayed into military commitment and capabilities, endogenous and exogenous determinants of levels of defence spending can be difficult to disentangle, and US defence spending encompasses defence elements that in many other countries are a civilian expenditure, notably the coast guard. The US, for instance, is estimated to comprise some 85 % of NATO's combat capacity. For the majority of NATO members—those already moderate in size—cuts are impeding their ability to sustain a full-spectrum warfare capacity and its deployment. Henceforth, the fiscal room necessary to maintain the extent of their global position and involvement, let alone adopt major new initiatives is becoming ever more constrained. The political demography of population aging is thus an intervening variable in projecting political, economic and military power: the consequences for collective burden-sharing in international security are that fewer allies are likely to end up having to do more with less (Haas 2011).

Globally, in the context of slowing economic growth, increased costs of labour, and the prospects of the crowding out of defence spending, no state or combination of states appears likely to overtake the United States' position of economic and military dominance. In fact, global aging is likely to extend US hegemony and deepen it, as these other states are likely to lag the United States (Rowland 2012). Demographic developments suggest that there is no other country on the horizon that is able to muster America's combination of innovation, economic growth, and low ratio of spending on capital versus personnel (which is key to military dominance on the high-tech battlefield of fourth generation warfare). Global population aging is thus likely to generate considerable security benefits for North America.

5 Collective In/Security: Supply and Demand

As much of the developing world transitions through historic population booms, the strain on governments' resources from national debt and the cost of aging populations has the potential to multiply systematically both the number of fragile states and the extent and depth of that fragility. Eventually, the aging problem in many developing states is likely to be as acute as for industrialized countries, but the former have the added disadvantage of growing old before growing rich, thus greatly handicapping their ability to pay for elder-care costs (Qiao 2006). If the strain on governments' resources caused by the cost of aging populations becomes sufficiently great, it may exacerbate systematically both the number of fragile states and the extent and depth of that fragility. Fragile states are prospective havens for organized crime and terrorism. The prospect of confronting more fragile states with fewer resources could prove the allies' single greatest security challenge of this century (Cincotta et al. 2003).[43] Already there is less capacity to realize other key international objectives, including preventing the proliferation of weapons of mass destruction (WMD), funding nation-building, engaging in military humanitarian interventions, and various other costly strategies of international conflict resolution and prevention.

At the same time, changes in population structure are prone to make the twenty-first century particularly unstable (Duffy Toft 2014a, b). Demographic shifts caused by the uneven global demographic transition will intensify by the 2020s and continue up through 2050. Trends whose implications are bound to prove particularly sanguine for the security environment include growing demographic disparities between (a) *nation-states*, e.g., the demise of the USSR and a declining Russia versus a rising Pakistan; (b) *age groups*, e.g., intergenerational conflict is countries with structural demographic imbalances, such as Afghanistan and Saudi Arabia; (c) *rural-urban groups*, e.g., urbanization in the Middle East and 'sons of the soil' violence sparked by conflict over land; and (d) *ethnic* or *religious* groups within states, e.g., solipsistic conflict conjured up by Hindu nationalists concerned about Muslim demographics in India, Zionists concerned about Palestinian population growth in the Occupied Territories, and conflict arising from demographic differentials between evangelicals and seculars in the United States (Diamond 1997; Dabbs Sciubba 2011a, b, 2014; Toft 2014a, b; Weiner 1978; Fearon et al. 2011; Brass 2011; Zarkovic 1997; Kaufman 2004, 2010; Goldstone et al. 2014). Each form of demographic disparity is associated with distinct political conundrums: interstate changes in population size and age structure affect the global balance of power. Unbalanced age (and sex) ratios tend to alter rates of economic growth, unemployment, instability, and violence. Urbanization engenders dislocations that have traditionally been associated with religious, ethnic, class, or nationalist movements. As urban growth outpaces national population growth by a factor of 1.5, the proportion of urban dwellers across the world is projected to rise to 70 % by 2050. In LDCs, where population growth is greatest, that equates to about three billion more people who will live in cities, 1 billion by mid-century in sub-Saharan Africa alone. While much attention has been focused on the growth of mega-cities, most of the urban growth is expected to transpire in secondary centers along migratory crossroads. Where the annual rate of urban population growth exceeds 4 %, the probability of civil conflict has been found to be 40 %; where the rate of growth is between one and 4 %, it is half that at 20 %, and where urban population growth is less than 1 % it is 19 %.

Urban migration is also likely to cause growing disequilibria among ethnic populations, as “sons of the soil” contend with an influx of other ethnic groups. Prominent examples where population differentials are already a driver of conflict include Israel, Lebanon and Nigeria as well as indigenous conflicts over land across the Americas and Oceania whose populations have some of the highest fertility (and migratory) rates in the world. Differentials in ethno-religious population growth set the stage for internecine violence, value conflict, or territorial disintegration. With global population concentrated overwhelmingly in fragile states, the growth in the world’s future labour force is occurring predominantly in fragile states with a weak ability to provide education, investment and jobs to ensure their productivity and socio-political stability (United Nations 2014).

Although the rate of global population growth is slowing, the impact is still staggering. As depicted in Table 4, the populations of 50 countries are projected to grow by a third, in some cases by two thirds, by 2025.

Table 4 Fastest growing countries 2005–2010 (at least 1 million people)

Country[a]	Annual Growth Rate (%)
Liberia	4.1
Niger	3.9
Afghanistan, **Burkino Faso**	3.4
Syria, Timor L’este, Uganda	3.3
Benin, **Palestine (occupied)**	3.2
Eritrea	3.1
Jordan	3.0
Burundi, **Tanzania**, **Yemen**	2.9
Chad, Congo (DR), **Gambia**, Malawi, **UAE**	2.8
Angola, Rwanda, Madagascar, **Sierra Leone**	2.7
Ethiopia, Kenya, **Senegal**	2.6
Guatemala, Togo	2.5
Kuwait, **Mali, Mauritania**, PNG, Zambia	2.4
Cameroon, Côte d’Ivoire, **Guinea**, Mozambique, **Nigeria, Somalia**	2.3
Guinea-Bissau, **Iraq**, **Pakistan**, **Sudan**	2.2
Ghana, **Oman**, **Saudi Arabia**	2.1
Honduras, **Libya**	2.0
Cen. Afr. Rep., Congo, Namibia, Nepal	1.9
Bolivia, **Egypt**, Gabon, Ireland, Laos, Paraguay, Philippines	1.8
Israel, **Malaysia**, Venezuela	1.7
Cambodia, Haiti, Panama, **Tajikistan**	1.6
Algeria, Colombia	1.5

[a] Countries with 50 % or more Muslim population in **Bold**

Source Department of Economic and Social Affairs

These are predominantly large, Islamic countries of 60 million people or more that are concentrated in sub-Saharan Africa, the Middle East and South Asia. With the demographic transition progressing more rapidly in the Middle East and South Asia, the challenges associated with population growth will be greatest in sub-Saharan Africa (Julia and Korotayev 2014). A youth bulge—a disproportionately large proportion of young people aged 15–29 among the adult population—puts countries at greater risk of civil violence and revolution, especially when characterized by unemployed young males. Countries in which more than 60 % of the population is under 30 have been shown to be four times more prone to civil war than countries with mature populations (Leahy et al. 2007). A low median age in the population may also delay the onset of democracy, and may make democratic gains difficult to consolidate and maintain (Huntington 1996; Urdal 2011; Cincotta and Doces 2011).

6 Conclusion

Never have there been as many people in the world. Never have there been so many old people. Never have they comprised a greater proportion of the population. Never have they been more affluent. And never have they wielded more political power. Such are the endogenous effects imposed by a historically unprecedented demographic horizon that is introducing considerable uncertainty into international interventions by virtue of being historically unprecedented. The rise in age of the median voter and the proportion of older voters is bound to affect public policy priorities. Older people tend to be more reliant on the state than younger ones. Not only do older voters thus have an incentive to resort to rent seeking, but also because of their advanced age they have an incentive to favour short-term payoff over long-term strategy.

Foreign policy rarely wins elections; domestic policy does. Ergo, social entitlement programs are likely to crowd out defence spending. Politicians are not just loath to curtail entitlement programs, electoral logic suggests that they are actually prone to expand them to appeal to this, the fastest growing cohort among the electorate. Stubbornly soft economic conditions further exacerbate the impact on defence spending as governments strive to balance their budgets by cutting defence. Yet, national defence and international instability tend to require a long view, which will be increasingly difficult to defend as the gambit of existential political payoffs for an aging population grows. The end effect is less overall capacity to intervene among allied countries.

Technological innovation goes some way toward harnessing the sort of efficiency gains that are more indispensable than ever to secure, maintain and augment collective security "productivity" in heavily constrained fiscal times. Robotics in military operations, whether cyborg "soldiers" on the battlefield or drones in the air, hold out considerable promise, at least insofar as the ability to reduce the labour intensity of collective security. But innovative military technology is exceptionally expensive, requires sustained patience over long development horizons, and an eventual political commitment to procure and roll it out. It is also neither clear nor obvious that such technological innovation necessarily reduces labour requirements. While military robotics may automate some functions previously performed by human beings, operators will remain indispensable to ensure strict compliance with international law, such as the Law of Armed Conflict, the constitutional and legal bounds within which armed forces in democracies operate, as well as military and professional ethics, national caveats, mission mandates and rules of engagement. Machines may perform functions, yet we are still far from the age where machines will be able to make the many and complex difficult judgments that encumber civil-military relations and, perforce, strategic planning, military operations and tactical decisions. Democratic citizens are unlikely to relegate such judgment calls to machines anytime soon. And in a tight labour market where the skillset such operators will need to have are increasingly at a premium and reflected in their ability to command hefty salary premiums, the fiscal gains from substituting capital for labour will be less than "technoptimists" might anticipate.

Demographic trends can become more sustainable, and the fragile states they affect more economically and socially resilient. On all those fronts broader and higher levels of education have widely been shown to be especially effective. City planning can enhance economic development and political stability to counter the effects of urbanization. Better management and protection of internally displaced people (IDPs), international refugees and migration to counteract their potentially destabilizing effects, especially in those fragile states that already shoulder a disproportionate burden of refugees, is in the interests of the countries of origin, the countries of destination, and the migrants themselves.

That is all the more important in the aftermath of Afghanistan, now that allied governments are morally, politically, and economically exhausted. Their interventionist malaise is at least partially conditioned by demographic change. Aging populations tend to be less predisposed towards war. As fertility rates decline, parents become disinclined towards risking the life of a child by going to war. At the same time, social citizenship obligations of the welfare state are increasingly crowding out defence spending, as evidenced by national debt loads and the difficulty experienced in realizing major military procurement. On the one hand, demographic trends posit rising demand for interventions while supply in US and allied capacity and political will is on the wane. On the other hand, most of the demographically destabilizing developments are occurring far from allied shores and are thus unlikely to pose an imminent or existential threat to the United States and its allies. For countries in the affected regions, however, especially the arc of Muslim countries stretching from North Africa through Pakistan, demographic developments pose a far more immediate or even existential threat. As a result, insofar as allied interests and theirs align, allies have a vested interest in getting used to unconventional partners. In light of mounting constraints allies will be facing to deploy on the one hand, and the probability that when they intervene, capacity to do so will be reduced, coalitions stand to benefit from participation by regional partners, not solely to maximize tactical effect, but for purposes of legitimating an intervention both domestically and abroad.

References

Anderson M (1996) British population history: from the black death to the present day. Cambridge University Press, Cambridge

Angenendt S, Apt W (2010) Die demographische Dreiteilung der Welt: Trends und Sicherheitspolitische Herausforderungen. Berlin: Stiftung Wissenschaft und Politik, 2010. http://www.swp-berlin.org/fileadmin/contents/products/studien/2010_S28_adt_apw_ks.pdf

Bloom DE, Canning D, Fink G (2011) Implications of population aging for economic growth. Harvard program and the global demography of aging working paper no. 64, 2011. http://www.hsph.harvard.edu/pgda/WorkingPapers/2011/PGDA_WP_64.pdf

Brass PR (2011) The production of hindu-muslim violence in contemporary India. University of Washington Press, Seattle

Cincotta R, Engleman R, Anastasion D (2003) The security demographic—population and civil conflict after the cold war. Population Action International, Washington, DC. http://www.populationaction.org/Publications/Report/The_Security_Demographic/The_Security_Demographic_Population_and_Civil_Conflict_After_the_Cold_War.pdf

Cincotta R, Doces J (2011) The age-structural maturity thesis: the impact of the youth bulge on the advent and stability of liberal democracy. In: Goldstone JA, Kaufmann EP, Duffy Toft M (eds) Political demography: how population changes are reshaping international security and national politics. Oxford University Press, New York

Culhane MM (2001) Global aging: capital market implications. Goldman Sachs Strategic Relationship Management Group, New York

Dabbs Sciubba J (2011a) The future of war: population and national security. Praeger International Security/ABC-CLIO, Santa Barbara, CA, p 2011

Dabbs Sciubba J (2014) Coffins versus cradles: Russian population, foreign policy, and power transition theory. Int Area Stud Rev 17(2):205–221

Dabbs Sciubba J (2011) Population aging and power transition theory. In: Goldstone JA, Kaufmann EP, Duffy Toft M (eds) Political demography: how population changes are reshaping international security and national politics. Oxford University Press, New York

Davidson J (2012) Explainer: this graph shows how NATO's military capability has evolved since 1949. Defence in Depth. 4 September 2012. http://blogs.cfr.org/davidson/2014/09/04/explainer-this-graph-shows-how-natos-military-capability-has-evolved-since-1949/

Duffy Toft M (2014a) Demography and national security: the politics of population shifts in contemporary Israel. Int Area Stud Rev 15(1):21–42

Department of Economic and Social Affairs (2014) World urbanization prospects. United Nations, New York

Diamond J (1997) Guns, germs, and steel: the fates of human societies. W.W. Norton, New York

Duffy Toft M (2014b) Death by demography: 1979 as the turning point for the Soviet Union. Int Area Stud Rev 17(2):184–204

Duffy Toft M (2003) The geography of ethnic violence: identity, interests and the indivisibility of territory. Princeton University Press, Princeton

European Defence Agency (2006) An initial long-term vision for European defence capability and capacity needs. Brussels

Fearon JD, Laitin DD (2011) Sons of the soil, migrants, and civil war. World Dev 39(2):199–211

Frey WH (2011) Racial demographics and the 2008 presidential election in the United States. In: Goldstone JA, Kaufmann EP, Duffy Toft M (eds) Political demography: how population changes are reshaping international security and national politics. Oxford University Press, New York

Friedman T (2014) Don't just do something, sit there. The New York Times. 26 February 2014. http://www.nytimes.com/2014/02/26/opinion/friedman-dont-just-do-something-sit-there.html?_r=0

Friedman BM (2005) The moral consequences of economic growth. Alfred Knopf, New York

Goldstone JA (1991) Revolution and rebellion in the early modern world. University of California Press, Berkeley

Goldstone JA (2011) A theory of political demography: human and institutional reproduction. In: Goldstone JA, Kaufmann EP, Duffy Toft M (eds) Political demography: how population changes are reshaping international security and national politics. New York University Press, Oxford

Goldstone JA, Marshall MG, Root H (2014) Demographic growth in dangerous places: concentrating conflict risks. Int Area Stud Rev 17(2):120–133

Goldstone JA (2002) Population and security: how demographic change can lead to violent conflict. Columbia J Int Aff 56(1) Fall, 245–63

Haas ML (2011) America's golden years? US security in an aging world. In: Political Demography, op. cit., pp 49–62

Huntington SP (1996) The clash of civilizations and the remaking of world order. Simon & Schuster, New York

Jackson R, Howe N (2011) Global aging and global security in the 21st century. In: Goldstone JA, Kaufmann EP, Duffy Toft M (eds) Political Demography: How Population Changes are Reshaping International Security and National Politics. Oxford University Press, New York

Jackson R, Howe N (2008) The graying of the great powers. Center for Strategic and International Studies, Washington, DC

Julia Z, Korotayev A (2014) Explosive population growth in tropical Africa: crucial omission in development forecasts—emerging risks and way out. World Futures 70(2):120–139

Janowicz M (1960) The professional soldier: a social and political portrait. Free Press, Glencoe, IL

Kaufmann EP (2011) Demographic change and conflict in Northern Ireland. J Ethnopol 10(3–4):369–389

Kaufmann Eric P (2012) Whither the child? Causes and consequences of low fertility. Paradigm Publishers, Boulder, CO

Kaufmann EP (2004) The rise and fall of Anglo-America. Harvard University Press, Cambridge, MA

Kaufmann EP (2010) Shall the religious inherit the earth? Demography and politics in the twenty-first century. Profile Books, London

Kaufmann EP, Toft MD (2011) Introduction. In: Goldstone JA, Eric PK, Toft MD (eds) Political demography: how population changes are reshaping international security and national politics. Oxford University Press, New York

Larrabee FS, Johnson SE, Gordon J IV, Wilson PA, Baxter C, Lai D, Trenkov-Wermuth C (2012) NATO and the challenges of austerity. Monograph 1196. RAND Corporation, Santa Monica

Leuprecht C (2014) Political demography of Canada-US co-dependence in defence and security. Canadian Foreign Policy J 20(3):291–304

Leahy E, Engelman R, Gibb Vogel C, Haddock S, Preston T (2007) The shape of things to come: why age structure matters to a safer, more equitable world. Population Action International, Washington, DC. http://www.populationaction.org/wp-content/uploads/2012/01/SOTC.pdf

Leuprecht C (2010) The demographic security dilemma. Yale J Int Affairs 5(2) Spring-Summer, 60–74

Leuprecht C Appease or Deter? (2011) The demographic structure of ethno-nationalist conflict. In: Goldstone JA, Eric PK, Toft MD (eds) Political demography: how population changes are reshaping international security and national politics. Oxford University Press, New York, pp 226–237

Leuprecht C (2012) The ethno-demographic structure of democratic consolidation in Mauritius and Fiji. Commonwealth and comparative politics. 50(1) 23–49 February

Leuprecht C (2010) Socially representative armed forces: a demographic imperative. In: Szvirczsev Tresch T, Leuprecht C (eds) Europe without soldiers? Recruitment and retention among Europe's armed forces. McGill-Queen's University Press, Montreal and Kingston, pp 35–54

Moskos CC (1977) From institutions to occupation: trends in military organization. Armed Forces Soc 4(1):41–50

Moskos CC, Williams JA, Segal DR (1999) Armed forces after the cold war. In: The post-modern military. Oxford University Press, Oxford, Chapter 1

OCED (2011) Providing and paying for long-term care, Chapter 2. http://www.oecd.org/els/health-systems/47884543.pdf

Qiao H (2006) Will China grow old before getting rich? Global economic paper no. 138. Goldman Sachs Economic Research Group, New York

Rowland DT (2012) Population aging: the transformation of societies. International perspectives on aging 3. Spriger Science + Business Media, Dortrecht

Teitelbaum MS (2014) Political demography: powerful forces between disciplinary stools. Int Area Stud Rev 17(2):99–119

United Nations Population Division (2014) World urbanization prospects: the 2014 revision population database. At http://esa.un.org/unup

Urdal H (2011) Youth bulges and violence. In: Goldstone JA, Kaufmann EP, Duffy Toft M (eds) Political demography: how population changes are reshaping international security and national politics. Oxford University Press, New York

Vanhuysse P, Goerres A (2012) Aging populations in post-industrial democracies. Routledge/ECPR European Political Science Series, Abingdon

Weiner M (1978) Sons of the soil: migration and ethnic conflict in India. Princeton University Press, Princeton

Williams C (2007) Service to country: personnel policy and the transformation of western militaries. MIT Press, Cambridge, MA

Williams C (2004) Filling the ranks: transforming the US military system. Cambridge, MA

Winter J, Teitelbaum MS (2013) The global spread of fertility decline: population, fear and uncertainty. Yale University Press, New Haven

Zarkovic Bookman M (1997) The demographic struggle for power: the political economy of demographic engineering. Frank Cass, London

Economic Security: An Analysis of the Strait of Malacca

Tyler Valdron

Abstract Following the outlining of a broad definition for economic security this chapter focuses on the trend of increasingly interdependent, complex economic systems and how they can be navigated. A framework is established where the risks related to economic security can be approximated as interdependent networks vulnerable to cascading failures. Scaling networks have characteristics that allow for a node-focused approach to security where the hubs of the network can represent the major units or hubs in the system, and to demonstrate the effectiveness of this perspective in economic security, a case study is provided. The case of Lloyd's of London and its intervention in the Malacca Strait will show how private actors who appreciate the criticality of node-based concepts in economic systems can apply such knowledge to their benefit. The effects of localized catastrophes on corporate markets are discussed as well, so as to demonstrate the link between macro and micro-economic nodes as well as how to identify economic nodes. The framework established and demonstrated will be useful for the decision making processes of experts in the field.

Keywords Economic security · Insurance · Piracy

1 Introduction

In many ways the emerging security issues of today can largely be traced to the increasing economic connectedness between different states and their citizens across the world, a phenomenon generally referred to as globalization. It is natural to wonder then, to what extent state economies are secure in this new global and interconnected society. Since the state security apparatus is traditionally focused in such a posture as to secure itself along and around its borders, threats that exist

T. Valdron (✉)
Carleton University, Ottawa, Canada
e-mail: n0rdl4v@gmail.com

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_8

outside of state borders may be more difficult to address. Yet we know that most state economies, particularly in the first world, are heavily dependent on business processes that exist outside of their state borders. Therein lies the modern challenge for states in securing their economies in a global economy, one that could be represented in the field of economic security. This chapter outlines theoretical perspectives and current trends within the field of economic security. Following a broad definition it focuses on the trend of increasingly interdependent, complex economic systems and how they can be navigated. A theoretical framework is established where economic security and the risks related to it can be best approximated as interdependent networks vulnerable to cascading failures. Specifically, scaling networks have certain characteristics that allow for a node-focused approach to risk management, where the hubs of the network can represent the major units or hubs in the system. To demonstrate the effectiveness of this perspective in economic security a case study is provided. The case of Lloyd's of London and its intervention in the Malacca Strait will show how private actors who appreciate the criticality of node-based concepts in economic systems can apply such knowledge to their benefit. The effects of localized catastrophes on corporate markets are discussed as well so as to demonstrate the link between macro and micro-economic nodes as well as how to identify economic nodes in the real world. The framework established and demonstrated here will be of great use in comprehending modern challenges in economic security and thus be useful for the decision making process of experts in the field.

2 Constructing a Framework for Economic Security

Engineers usually distinguish between security and safety features of a structure by noting that safety features are those that are required for the building to provide a standard level of service while causing no undue risk to the users, while security features may be added to address the risk of damage and destruction to the structure represented by intentional attacks, illegitimate access or use, and extreme but unlikely circumstances, such as an unexpected natural disaster (Control Global 2014). Translating this concept to other fields will be useful given this is a discussion that will attempt to define new concepts in non-traditional fields of security. As it will be explained, economic security can be defined more specifically than just the potential for bad things to happen to the economy. This tighter definition will allow for better focus when experts approach the subject of economic security.

Economic value is a measurable quantity compared to concepts of security. The most straightforward method of measuring the results of good economic security from the state perspective is to look at the changes in a state's economic metrics over time. There are several metrics to work with. Annual Gross Domestic Product (GDP) is a measure of the value of all the goods and services produced within a country's borders per year. This first metric can be contrasted with the annual Gross National Product of a state, which measures the total value produced by all citizens of the state globally minus domestically located overseas residents. This contrast is a good indication of the changing perspectives in economics caused by the phenomenon of globalization. Borders may no longer be the best way to separate what is of one state but not the other, and so on. Another important measure that captures the change in the economic value of a state is economic growth. Traditionally, this is a metric that is based on the change in GDP over a year. Finally, measures of the indebtedness of an economy are increasingly cited as a threat to overall economic wellbeing, though to what extent and how are the subject of much debate (Reinhart 2009).

Delineating as to what is economic security, as opposed to economic risk, is a key discussion. Fortunately, there is an industry in existence that has for hundreds of years concerned itself with this very distinction. The Insurance industry contrasts pure risk with speculative risk in such a way as to parallel the distinctions that define traditional security issues. Speculative risk is described as risk where there is the possibility of loss or gain, whereas for pure risk, there is only the possibility of loss or no loss. Insurance manuals make this distinction because the contract of insurance upon which the industry is based is intended only to address the possibility of loss due to pure risk. Thus, one cannot insure an investment into a new company that then fails to sell because there was the possibility of sale and profit. Rather, one can only be covered by insurance for such occurrences as theft, or fire, which simply destroy or disrupt economic value and assets with no opportunity for gain by the owner of said assets. Insurance is only intended as a way to indemnify the insured from loss due to pure risk, that is, to restore to them what value was lost due to pure risk, and not a penny more.

Natural Catastrophes produce negative effects on average for the short to medium term (Munich Re, University of Wurzburg). Though it is sometimes suggested that reconstruction after a disaster can act as a stimulus for local economies, it is also found that the stimulus effects from reconstruction are outweighed by capital destroyed in the event. Insurance relationships have a preventative component in regard to dealing with natural disasters and other threats due to the insurer's exposure through their clients, as well as the obvious enhancement to recovery through financial support (Bank of International Settlements). The Bank of International settlements finds that well insured economies only suffer short to medium effects in terms of economic growth, but where the economy is uninsured there can be a permanent growth deduction of close to two percent. The Bank of International Settlements study in question covered 2476 natural disasters across 200 countries. Regional Risk Pooling Organizations such as the Caribbean Catastrophe Risk Insurance facility are helping developing countries not only financially address disasters directly, but also become more appealing to developed catastrophe investors such as international reinsurers. Top reinsurers best operate under large insurance treaties where there is enough data about disasters in the area to take advantage of economies of scale. Of particular interest in regard to economic security, Critical Infrastructure has been described by the US government as key infrastructure in society that is required for all other aspects of society to function. What sectors are considered critical infrastructure varies by country. Being that a key finding in the investigation by the US government surrounding the 9/11 attacks was that though modern society is incredibly dependent on its critical infrastructures, these assets are by over 80 % owned privately, private insurance solutions may be more familiar to the critical infrastructure sectors.

One could define state economic security as the art of protecting a nation's economy from threats that represent pure risk as opposed to speculative risk. Both pure risk and speculative risk can cause measurable damage to the economy in the form of decreased GDP, GNP, and future economic growth. An example of speculative risk causing a decrease in GDP would be the collapse of an important state enterprise due to bad investments. Though the investments in this example caused an economic loss, the investments were presumably still made with the intention of creating profit and so this is a loss due to speculative risk, as an insurer would describe it. An example of loss due to pure risk, which would then fall under the jurisdiction of our future economic security experts and policymakers, could be a terrorist attack on a major financial center such as with the 9/11 attacks where the financial operations and assets of the United States and indeed the world were disrupted.

The challenge with modern economic security, it would seem, is that states seem to have less and less control over their economies, whether it be privation of infrastructure at home, or the spread of capital and economic interdependencies globally. Using our constructed definition of economic security, it is fairly straightforward to identify cases where there are linear actions with intended effects. For example, the bombing of Dresden during World War 2 was a military campaign brought on by the Allies with the specific intent of weakening Germany's industrial capacity through the direct destruction of their factories and other built of assets support the war economy. In this historical case, the attacks by the allies on Germany represent no direct prospect of economic gain and thus speculative risk, rather, the challenge of defending the city from bombing was simply a matter of saving as many lives and industrial materiel as possible. Thus, the efforts on Germany's part to defend against the allies were a matter of economic security.

The modern day challenge of so-called economic security is that the globalization of the world economy ensures that linear economic security cases such as the Bombing of Dresden are rarer, and instead we faces nebulous economic risks with unclear actors, boundaries, and effects. In the case of the 9/11 attacks, the conduit (vector) (McDougall and Radvanovsky 2008, Sect. 2.3: 13) of attack used was that of private air transport infrastructure that was not controlled directly by the government, and the most memorable targets of the attack, the world trade center towers, were a center for private finance. The attackers did not fall under the banner of a single state, and their desired effects on the economy were not linear. Indeed, many of the companies that suffered the worst from the attacks rallied well in terms of profit after the disaster, and the entire global financial infrastructure was not fully disrupted for a significant period of time. Moreover, most of the companies suffering damage were not only owned by US citizens, meaning the losses were also not contained to the United States' GDP and other measures. The Northeast Blackout of 2003 represents another example of an economic security issue that was not contained to a single state. The power outage originated in Ohio but affected all of Southern Ontario as well as other US States, disrupting local economic activities directly and indirectly. More than just confusing what were once simple issues, emerging theories in the realm of international politics and economy suggest that globalization exerts a powerful set of incentives in regard to state behavior that increasingly shape world affairs. Evidently, a new, less state-centric framework is needed when exploring economic security issues in an era of a globalized economy.

Many in the field of security have addressed these framework challenges by replacing a state-centric perspective with various hub and spoke models. These models focus on the clustering of interdependent assets and activities in need of security, referred to as nodes (McDougall and Radvanovsky 2008, Sect. 2.3, p. 12), as well as the conduits of transportation, energy, and communication between them. Given that economic value derives from these assets and activities, placing a similar focus on systems of nodes and the conduits between them is logical. In a small scale example, a factory producing goods of economic value could be considered an economic node. It would generally be dependent on conduits such as marine and land transportation infrastructure that bring labor and material to the node, as well as distribute its final product outward from said node. Importantly, this economic node can only operate with the support of other nodes whether they be economic, such as the fellow economic nodes that produce needed materials, and the energy nodes that ensure the factory is powered and operational. Due to these many interdependencies, the failure of one node or even conduit in a system quickly leads to more failures, the effects of which will then cause even more nodes to fail, and so on. This phenomenon is usually referred to as a cascading failure within a system. Though originally conceived for use in the realm of computer network security, the concept of a scaling network (Lewis 2014) has also begun to see use in other fields and will be useful in regard to economic security. A Scaling node is a node where there has been an exponential rise in the number of other nodes dependent on it such that its failure would have notably dire consequences in the forum of cascading failures. Thus, in this framework for the study of economic security from a state or global perspective, our basic units are economic nodes such as cities or large industrial complexes, and they are glued together by many different kinds of conduits such as road networks and global sea lanes. If an economic node of massive economic value and with scaling properties in terms of the number of other nodes dependent on it were simply to be wiped off the map, the adverse effects may be felt by many states around the world due to the phenomenon of cascading failure among nodes.

A construct that may be helpful for further study is Value at Risk (VaR) (Knight and Pretty 1996). Value at Risk theory in particular provides categories for companies and how they respond to major shocks. Recoverers are those companies that respond well to disasters, and non-Recoverers, being those that do not respond well to disasters. This is measured based on how share prices perform following such shocks to the company. A company’s public share price performance over a time series is public information, which allows for more open research. Working back to the findings that state economies that do not deal well in damage from natural disasters and other macro shocks, we can see how permanent growth losses on the macroeconomic scale translate onto the microeconomic scale. When local industries are unprepared and not sufficiently resilient, they are less likely to fall into the "Recoverers" category according to VaR theory, and so they suffer long term stock losses due to falling investor confidence in addition to the asset losses. These microeconomic results then combine to be measured as an overall economic growth loss on the macroeconomic level. Furthermore, this theory demonstrates the key role psychology has to play on the microeconomic level, because investor confidence can turn a small loss into a large loss, or even a loss into a profit if, after a strong response to a shock to the company, investor confidence surges. The fact that the psychology of fear and excitement can play so directly into the realm of economic security even at microeconomic levels is one of the reasons why the traditional security field and economic security studies can learn from each other.

Having established the units of value in need of protection for a framework of economic security, there must also be concepts of the threats to be protected against. As previously discussed, insurers have neatly established some of these concepts and so for the purposes of this framework, the threats are represented by pure risk and *not* speculative risk. To break pure risk down further, it is the potential for loss, in this case economic loss which would show on the state level as a loss in assets and potentially a loss of growth or potential growth in an economy. Risk itself is derived from the variables of probability and severity. Probability is the likelihood of the loss occurring, and severity is the amount of damage to economic value it would cause if it did occur. Defining things further, severity of losses in the realm of economic security can be measured as losses to the GDP or GNP of a state, or loss of growth as well as potential/predicted growth.

3 The Case of Lloyd's of London and the Strait of Malacca

As reinforced in the construction of the definition of economic security, the global economy is subject to certain geographical chokepoints of trade and logistics (Rodrigue 2004), and a threat that can disrupt these chokepoints is also a threat to the economy of the major nations of the world. These are the nodes to be studied in international economic security. The Malacca Strait is one such node, particularly in regards to petroleum supplies (Rodrigue 2004). The lack of security cooperation in the Malacca Strait between the littoral states whom have jurisdiction over the area was of great concern to the United States in the aftermath of the 9/11 attacks given the history of piracy and terrorism in the region (Weitz 2008), and this lack of cooperation could be modeled a threat to economic nodes in the area. Having recognised this threat to global shipping and the US economy, there were repeated attempts to reconcile and coordinate efforts between Indonesia, Singapore, and Malaysia as well as other states active in international security, but during the period of time between the 9/11 in 2001 attacks and 2005 they were relatively unsuccessful. When Lloyd's of London[1] quietly put the Strait of Malacca on their war risk insurance listing, the desired security cooperation between these littoral states improved drastically over a three month period (Weitz 2008). This has left decision makers wondering how Lloyd's succeeded where conventional US foreign policy efforts failed. In this case, not only do we see the impact a threat to the economic security of a nation or several nations through a major node, but also how these threats motivate decision-making.

Why was the international insurance group, Lloyds of London, more effective in motivating security cooperation in the Strait of Malacca between the littoral states of Indonesia, Singapore, and Malaysia? How can economic security decision makers learn from this case so that they can better address future challenges? Transnational insurance actors like Lloyd's of London have unique and potent ways to influence state policies as a result of their importance to the economy and how international corporations decide to treat risk. If states wish to secure their economies from non-traditional and globalized threats, they will need to appreciate this more corporate perspective.

A brief summary and initial analysis of the events and actors surrounding Lloyd's involvement in the improved security cooperation between the littoral states of the Strait of Malacca, Malaysia, Indonesia, and Singapore, will be provided as part of the case study. The case discussion will explore how Lloyd's of London demonstrated that even slight increases in the shipping insurance rates, which they are able to suggest to the rest of the international insurance industry, can have serious impacts on the businesses in regions affected such that they will pressure their governments to take action to appease Lloyd's concerns over security threats. In addition, when it comes to addressing security concerns resultant from insurgency and terrorism, it will be shown that the effective strategy of cooperation between security actors and empowerment of the local security institutions is better approached by a non-state transnational security actor such as Lloyd's of London rather than International US security actors. This is due to the concern local states have that their sovereignty would be eroded as a result of US intervention. It will also be demonstrated that whereas US security interventions into international security problems such as the transnational criminal networks operating in the Malacca Strait can have the potential to destabilize and escalate the situation, the buildup of local financial institutions and associations fostered by the involvement of international insurance groups in the region will foster collaboration and stability in the region. Policy implications for the US will be provided as well. Exploring how this systems of economic nodes and conduits, particularly the key conduit that the Strait of Malacca can be modeled as, was interacted with by different state and

[1] Lloyds of London is a historic nexus of specialised insurance (a financial product that reimburses clients financially for certain potential losses) underwriters, brokers and experts that together form on world insurance market that still dominates specialised and large risks in particular, including maritime insurance (Weitz 2008).

non-state actors will be helpful in solidifying the sense of a concrete model for economic security by attaching the models to a real security case.

The Lloyd's of London Joint War Committee's (JWC) goal is to serve the interest of its underwriters by providing information on risks. With this information, individual underwriters can judge for themselves whether or not to adjust insurance rates in response (Weitz 2008). The JWC's risk classifications have been known to result in large increases in insurance costs for vessels traveling through high risk regions, which can cause those shipping companies to avoid the high-risk classified areas in an effort to reduce costs (Weitz 2008). The fact that this has been the case also demonstrates the significant effect a non-state actor can have on an individual state economy, even unintentionally. Given that 80 % of global trading goods are at some point moved by sea (Weitz 2008), this means that the influence of JWC war risk evaluations is wide-reaching. More specifically, one third of all world trade and one half of all oil shipments pass through the Strait of Malacca (Weitz 2008) which makes it the perfect model of a crucial node for economic security where insurance premiums are an important aspect of the business.

Transnational actors can generally be divided into two groups: those that specifically intend to influence the policy of nations, and those that may not intend to influence the policy of nations but may do so indirectly as a result of their actions (Weitz 2008). Insurance companies and their associations fall into the latter category in that their goal is not understood to be the changing or directing of public policy, but rather to profit through legitimate business relating to the insurance industry. Lloyd's of London therefore does not release a list of war risk classifications with the intent of shifting security policy, but simply to better inform the business of marine insurance underwriters.

Following mass insurance losses from the 9/11 attacks in the US, the JWC decided that it should no longer base its war-risk listings on retrospective events and analysis (Weitz 2008). Previously their risk classifications were updated methodically following major risk and loss events, but after 9/11 this method was changed to one where the JWC attempts to predict areas of future risk, a preventative strategy (Weitz 2008). When the JWC added the Strait of Malacca to its list war risk areas on June 20, 2005 (Weitz 2008), it was exercising this new preventative approach to its mission of informing marine underwriters of risk. The reaction from the maritime shipping industry was immediate, with many calls for a re-evaluation, but more notable was that Lloyd's and the JWC were quickly contacted by the British government.

Lloyd's was informed that the governments of Singapore, Malaysia, and Indonesia had all made official complaints to the British government over the listing of the Malacca Strait as a war risk area (Weitz 2008). In August of 2005 a joint public statement from the foreign ministers of Indonesia, Malaysia, and Singapore was issued emphasising their disagreement with the war risk area classification considering their existing efforts to ensure maritime security in the region (Weitz 2008). The classification had already resulted in insurers charging an addition 0.01 % of the value of each vessel for their policies, a significant additional expense (Weitz 2008). Despite mounting criticism from both industry and government, the chairman of the JWC issued an unapologetic statement, outlining that “the only thing that will change our minds is when our security advisers say there has been a change in the region and the Malacca Strait is made safer. There is no evidence of that happening” (Weitz 2008: 49). Furthermore, the security advisers to the JWC maintained that existing and even future increased security measures by the littoral states would not be sufficient unless the three governments of Singapore, Malaysia, and Indonesia cooperated closely in executing their security programs (Weitz 2008).

That specific demand was one in which other international actors, in particular the US, had tried and failed to enforce in the past. In the aftermath of the fall of the USSR at the end of the twentieth century, the cooperation of states in South East Asia towards greater maritime security was not well adjusted to the modern threats of international crime, piracy, and terrorism (Weitz 2008). The most progressive policy in the area in regards to maritime security cooperation in the Strait of Malacca was launched in July 2004, where the littoral states set up trilateral coordinated maritime patrols. Though this was the best program in the direction of cooperation at the time, it was fundamentally flawed because the historical distrust and competition between the littoral states meant that they were too sensitive about their sovereignty to allow for hot pursuit of targets during these patrols (Weitz 2008).

In 2004, the United States brought forward the Regional Maritime Security Initiative (RMSI), an initiative that was intended to increase information sharing and cooperation between security forces in the region (Weitz 2008). Though promising in concept, the project quickly fell apart due to suspicion of US military intervention in the region, especially given the recent US invasion of Iraq. RMSI received widespread opposition from the littoral states and the US had scuttled the project completely by 2005 (Weitz 2008). Another cooperative initiative forwarded by Japan, the Regional Cooperation Agreement on Anti-Piracy (ReCAAP) attempted to unify efforts in combating piracy, but fell victim to similar paranoia and sovereignty concerns when it was first signed in 2004, with the key states of Indonesia and Malaysia both refusing to sign the agreement (Weitz 2008). Even with the added incentives provided by Lloyds in 2005, the US attempts to foster cooperation in the region fumbled again in February 2006 with the Alameda summit. It was decided initially that the summit would be for countries that depended on the business from the Strait of Malacca rather than the littoral states themselves, and by the time that the obvious flaw of excluding the littoral states was corrected by inviting them as well, Malaysia had refused to attend out of insult. In the end, the summit was re-framed as another attempt by the US to infringe upon the sovereignty of the local littoral states (Weitz 2008).

Having failed to have the war risk rating removed by diplomatic means, the littoral states and local industry groups took action to satisfy the JWC and have the war risk rating for the Malacca strait removed on Lloyd’s terms. Within the first three months, Indonesia had made significant reforms and expansions to its naval presence, and the littoral states had arranged for major improvements in cooperation and addressed long-standing sovereignty concerns during the Batam summit. In addition, full joint air patrol operations had been launched through the Eyes in the Sky program where each aircraft on patrol contained officers from all three littoral states (Weitz 2008). Though 38 pirate attacks had been reported in the Strait of Malacca during 2004, by the end of 2005 only 11 had been reported, representing a steep decline (Weitz 2008). Following more lobbying by the littoral states and maritime industrial associations, the JWC issued a statement recognizing the increased cooperation in security in regards to the Strait but decided not to change the risk rating, indicating that it was hopeful that current results were indicative of "a favourable long-term trend" (Weitz 2008: 50). The JWC also stated that the new cooperative programs initiated by the littoral states were moving the situation in the right direction, but that the programs has not yet resulted in a reduced risk for the area (Weitz 2008).

Ultimately, Lloyd's of London would go on to revise their list of war risk areas three full times before finally removing the Strait of Malacca upon a fourth revision, released on August 7th, 2006 (Weitz 2008). The Chairman of Lloyd's of London, Lord Levene, congratulated the littoral states for improving security in the Strait of Malacca, noting that:

> It is a great tribute to the Government of Singapore and the other littoral states and other supporting countries that such rapid and effective action was taken that the [Joint War] Committee decided in August that [its] ruling would be rescinded (Weitz 2008: 52).

In the aftermath of the favorable revision to the war-risk list, state officials from Singapore, Malaysia, and Indonesia made repeated public statements that the removal of the Strait of Malacca from the list was evidence of significant security reforms and increased security cooperation, with pledges to continue the progress (Weitz 2008). Interviews with officials from the littoral states consistently supported the idea that the Lloyd's war risk rating was the direct impetus for the progress (Weitz 2008).

A key point of analysis from this series of event is that Lloyd's of London and the JWC, though initially releasing their list of war risk areas unilaterally as they always had, found themselves bargaining directly over security with the littoral states of Indonesia, Singapore, and Malaysia. The littoral states initially attempted to change the situation by interacting with the British Government, but when this failed to produce results they resorted to appeasing Lloyd's directly. The JWC was not lobbying the littoral states for policy change in the traditional sense; if anything the littoral states were lobbying Lloyd's and the JWC for insurance policy change. Weitz (2008) supports this perspective, noting that although the increased security cooperation between the littoral states was the trend the JWC produced, it can also be argued that the interactions between Lloyd's and the littoral states also represented cooperation between international actors. This in turn is a good example of how a system of economic nodes with many state stakeholders can twist the policy of nations towards it and above more traditional geopolitical concerns and rivalries, when there are threats to these nodes and by extension their individual economic security postures.

The case of Lloyd's intervention in the Strait of Malacca and the subsequent shifting of local security policy to appease the JWC by the littoral states of

Singapore, Malaysia, and Indonesia demonstrates that transnational insurance actors have distinct methods of shaping the policies of states. Dependence on international trade chokepoints such as the Strait of Malacca represents a strategic vulnerability (Deutch 2006) that can be exploited by threats whether they be other states or terrorists who may seek to disrupt or negatively influence these trade nodes. The US along with other states, in attempting to mitigate this risk in the case of the Strait of Malacca, was inhibited in improving security in the region directly or through the littoral states due to local concerns over sovereignty and the thought of a disruptive US military intervention. Jurisdiction and sovereignty disputes continued to block effective security cooperation efforts between the littoral states themselves as well (Weitz 2008). Rapid improvement in the area of security cooperation only happened after Lloyd's provided a direct economic incentive for the littoral states to cooperate. Lloyd's threat to the viability of the Strait of Malacca as a marine transportation conduit for the international system of economic nodes it served was felt more than more traditional diplomatic prodding efforts made by the United States.

Though both the US and Lloyd's stood to benefit from increased security in the Strait of Malacca, Lloyd's as an international actor had distinct options in how to achieve such a result. Specifically, the JWC war risk rating applied a pressure that was very important to the littoral states, a trade based economic pressure. The US applied diplomatic and military pressure, and this was not well received by the littoral states because they were worried about the impact of such initiatives on their sovereignty and potential disruptions resulting from direct intervention from a world power. In contrast, Lloyd's involvement did not represent an obvious threat to the sovereignty of the littoral states, and so was not met with the same prejudice and suspicion that similar suggestions by a state such as the US might be met with. Furthermore, the intervention by Lloyds re-framed the security issue of the Malacca state into one that was more tolerable for the littoral states to work with. The JWC only cared to address the economic risk facing maritime insurers and their clients and thus other states including the US were able to lobby from a new perspective where instead of suggesting that they would involve themselves in the improvement of local maritime security directly, that they are instead clients and users of the Strait and thus requesting greater service in the area of security, service which the littoral states could provide directly in their sovereign territory. This service and client based perspective generated because Lloyd's was not seen as a state and competitor who could interfere with the affairs and sovereignty of the littoral states. For the very reason that Lloyd's and other insurance actors are not seen as equal sovereign states by other states they operate in, they are able to bargain over policy relatively inoffensively compared to if the US were to attempt the same thing.

Though insurance companies are generally understood to take on the role of managing risk on behalf of their clients, to do this effectively they are able to also take on a "performative" role (Lobo-Guerrero 2012a, b: 78) where they actively influence and shape the security of global commerce. Rather than simply covering clients for their losses, they are incentivized to directly influence and contribute to the international security environment. In doing so they are able to discretely and unilaterally define what is acceptable and what is not within the realm of global shipping and thus the world economy that is ever so dependent on it (Lobo-Guerrero 2012a, b). The insurance industry has succeeded in transforming uncertainty into a tradable, marketable substance (Pierides 2014) and this concept is used to enable the fusion of commercial incentives with the forceful security capacities of the conventional state (Pierides 2014). This very fusion can be found in the case of the Lloyd's involvement in the improving of security cooperation among the littoral states in the Strait of Malacca. The commercial pressure provided by Lloyd's was a much more compatible vehicle to effective change compared to the diplomatic pressure of the US and other powers. This is a study of the effectiveness of different actors within the realm of economic security, which will be expanded on later.

Erosion of sovereignty due to foreign interference is not simply a theoretical concern to states, it is a well-studied phenomenon that is known to make counterinsurgency a difficult proposition. There are four major paradoxes that inhibit the success of counterinsurgency campaigns (Branch 2010). The first paradox, between the need for effective command structures provided by foreign world powers such as the US, and the need to devolve power to the local authorities for an effective counterinsurgency campaign, is well represented in the case of the Strait of Malacca. Direct US intervention in the Strait of Malacca was seen as problematic because it would interfere with the legitimacy and ability of the local security forces to secure the Strait, but it was also evident that the littoral states were in a political deadlock that prevented effective counterinsurgency by local authorities. The involvement of Lloyd's circumvented the political deadlock and concerns over sovereignty by framing the situation as one where clients and users, such as the maritime shipping clients represented by Lloyd's, needed increased security service from the littoral states so that business could continue. Once this new perspective was established, new security programs and cooperation initiatives that the US and others had previously attempted to provide were able to permeate through to the littoral states. The second paradox (Branch 2010), between the delivery of reform and repression, is somewhat represented in the case of the Strait of Malacca because the involvement of Lloyd's quickly drew the involvement of the various local commercial stakeholders as well as the three littoral states, allowing for more effective reform through transparent and informed negotiations. Though the war risk listing was not directly related to the level of violence perpetrated by the various stakeholder states, the request for greater security cooperation between the littoral states incentivized more joint solutions between the stakeholders as opposed to suspicion and sabre-rattling. The ability of Lloyd's to bring commercial stakeholders to the table also helped circumvent the third paradox between reform and civilian grievances in counterinsurgency campaigns (Branch 2010) because very direct incentives for civilian stakeholders to participate in a solution had been provided by Lloyd's.

The fourth paradox noted by Branch and Wood (2010), the possibility of a legitimate insurgency, is not necessarily addressed by Lloyd's solution to the security conundrum in the Strait of Malacca. This paradox may serve as a critique of the effectiveness of international insurance groups in their ability to resolve counterinsurgency problems because there are no obvious incentives for the insurers to recognise the insurgents, and this certainly was not the case in the Strait of Malacca. Lloyd's simply insisted on more effective security and counterinsurgency and thus its solution did not address any of the root causes of counterinsurgency. They note that one source of failure when it comes to the intervention of international insurance actors in security situations relating to counterinsurgency can be "taking the world as exogenous" (Greenhill and Staniland 2007: 407) wherein counterinsurgent forces often make the mistake of assuming that the same tactic will have the same effect at a different time in the same campaign, or in a different campaign entirely. In the case of insurance actors, their ability to intervene and the way in which they do it is limited as can be their perception, bound by goals of profit. Another source of failure according to Greenhill and Staniland comes from the "privileging technocracy over strategy" (Greenhill and Staniland 2007: 413) and this relates to insurance actors because from this perspective they could be argued to be biased towards technocracy due to corporate emphasis on general best practices, and a common reliance on actuarial risk analysis (Pierides 2014).

Another argument supporting the effectiveness of international insurance actors such as Lloyd's of London in shaping security policy derives from the fact that the intervention in the Strait of Malacca emphasized cooperation between the littoral states for increased stability, as opposed to intervention against the terrorist threat that was advocated by the US (Weitz 2008). Though the aforementioned critique of the intervention of insurance actors in counterinsurgency campaigns noted that insurance groups are unlikely to be motivated to address root causes of an insurgency, this lack of interference could be argued to prevent escalation and destabilization. It is well known that violent intervention into the international drug trade has largely served to increase violence in the area while failing to eliminate the drug trade (Werb et al. 2011). Such a result in the Strait of Malacca would be disastrous for all parties given its status as an economic chokepoint. The incentives provided by the JWC emphasised deterrence and security cooperation where the goal was to increase trade security rather than eliminate piracy (Weitz 2008). This solution was more suitable and less disruptive than a drug war style intervention (Werb et al. 2011) directed by the US against terrorism and piracy in the region would have been. The contrast between these different security solutions is put into a more understandable context if the framework for economics security is used. By understanding that the major threat in this case was to economic security, safeguards and security responses tailored to preserving and even promoting economic prosperity must be used as opposed to more traditional security approaches. At the heart of these global trade systems of conduits and nodes lies a need for sufficiently open borders and sufficient trust for mass trade, and so security efforts that hamper open trade may do more harm than good. Insurance relationships attempting to address economic security issues provide good examples of these more sensitive efforts.

No region or political system in the world has been able to prevent the emergence or effectively suppress the operations of organised criminal groups, and the pirates operating in the Malacca Strait are no exception. The fact that the incentives for cooperation and deterrence offered by Lloyd's in the Strait of Malacca are less likely to disrupt stable and less violent criminal networks serves as an argument in their favor, at least in terms of the preservation of stable trade in the region. On the other hand, this point can also serve as a critique of their methods because new waves of terrorists or violent crime groups may not be as concerned with maintaining a stable financial situation in the region (Shelley 2004).

Looking at the success of the intervention of Lloyd’s of London and the JWC in increasing maritime security cooperation in the Strait of Malacca between the littoral states of Indonesia, Singapore, and Malaysia compared to parallel failures by the US to achieve similar goals in the region, it is fair to say that greater consideration to the activities of transnational insurance actors should be given by US policymakers. Weitz’s seminal work (2008) on covering the details of this series of events has similar conclusions, noting that marine insurance is a “potential catalyst” (Weitz 2008: 2) for the promotion of cooperative international security programs, further speculating that actors like Lloyd’s of London could support or supplement more conventional diplomatic efforts.

Lloyd’s of London arguably has distinct and effective methods of influencing the security policy of states, and its methods may support better security in areas such as the Strait of Malacca where insurgency and criminal organizations are causing concern. The policy implications of these arguments are that insurance actors could be instrumental in fostering desirable development and security outcomes to the US in regions otherwise hostile to direct US intervention. The actions of an international insurance group can be modeled as those of a transnational actor engaging at the same level as states. Understanding this, state actors wishing to succeed in portfolios sensitive to fields insurance groups act in (such as development, trade and security) should make new efforts to better understand these organizations and their effects. Interference or needless regulation of the industry may make policy implementation more difficult, for example when the increased insurance rates for shipping in the Strait of Malacca enraged the industry community and thus made the littoral state`s pursuit of a sovereignty first security policy much more difficult. On the other hand, policymakers could be enabled by engaging with insurance corporations directly on security issues, or taking them into account as stakeholders when implementing new policy. Though not directly, the desire of US policymakers to increase security in the Strait of Malacca was ultimately enabled by Lloyd`s and the JWC.

4 Applying the Economic Security Framework

Setting aside the more general lessons learned from the Malacca case study, the framework for economic security established here provides further perspective. First, let’s look at the economic structure of the system being studied. The Strait of Malacca itself is a conduit as described in the introduction. Specifically, it is a marine transportation conduit and one of massive scale with roughly 70 thousand ships passing through it each year (Qu and Meng 2012). It connects so many major economic nodes to each other that there are few major nations that would not feel the effects of any problems that threatened the strait. Thus, for the sake of modeling, one could assume that this conduit, that is the Strait of Malacca, is of such importance that all major states with stakes in the area would consider a threat to it as a threat to their economic bottom lines. Certainly, there is a whole other discussion to be had about relative losses between different stakeholders, but that is a study as much psychological and strategic as material such that it would require much more sensitive information on part of the decision makers. In which case, the threats that might disrupt the Strait of Malacca as a conduit are not states, and probably transnational in nature.

In the case study, there are several threats to the conduit. First, there was the threat of piracy, where ships might be attacked and besides the direct value lost from stolen assets, fear on part of the merchants would no doubt be bad for business. This threat in theory would scale with the popularity of the conduit in terms of use, though when it comes to transnational crime there are many factors as discussed in the case study. Second, there was the threat of terrorist attacks in the area as declared by the United States at the time, specifically, that South East Asia was to be the second front for the War on Terror. These potential attacks threatened to be even more damaging to the effectiveness of the Strait of Malacca as a conduit than the historical piracy because the goal of the attacks suggested more indiscriminate damage as well as, unsurprisingly, more fear caused in the area. Furthermore, the government response to such incidents, if similar to that of the United States following 9/11, could be heavy handed and restrictive to trade flow, which, naturally, would also be bad for business and the effectiveness of the conduit itself, as well as local receiving nodes. Finally, the actions of Lloyd's of London in declaring the strait unsafe could itself be construed as a threat to the economic security of stakeholders in the area. In the same way that The United States increased security due to perceived threats following 9/11, Lloyd's of London increased its own security measures and that of the industry by suggesting higher insurance rates for shipping the Strait of Malacca. This loss of confidence in the security of the conduit had a cascading effect in the form of increased insurance rates which in turn was perceived as an economic threat by stakeholder nations who acted to appease Lloyd's security experts. What is of course most interesting in the case study was that when it came to threats that motivated action on part of local security actors, the United States construed threat of terrorism in the Strait of Malacca and South East Asia was not as motivating as the Lloyd's directed threat of increase insurance premiums. Our framework for economic security helps explain this. The littoral states of Singapore, Malaysia and Indonesia who represented the local security actors were much more threatened by loss of economic growth from insurance premiums than potential terrorist attacks and ongoing piracy attacks, as their economies and modeled economic nodes of significance were much more sensitive to increased cost in business compared to the threat of terrorist attacks. Looking at their economic node structures, these countries are particularly dependent on maritime transportation conduits given their statuses as island nations.

Another key area of study is in regard to the actors and how they relate to the economic system of nodes in question. In following with the theme of international security, simply evaluating these systems in terms of state actors quickly becomes limiting. The War on Terror, which continues to date at the time of this writing, is evidence of recognition of this at the level of state actors. International crime groups as well as local ones can have real measurable effects on economic nodes. They may, for instance, threaten the security of a node or conduit through direct damage or vandalism, or indirect violence between multiple crime groups. They may also be a cause of corruption within local nodes which in turn hurts the economic bottom line. Terrorist groups in the proper sense of course also threaten on the level of economic security. The attacks of 9/11 on the World Trade Center Towers were attacks on an economic node in the most direct sense. The security fallout in the aftermath also had measurable economic effects. For those that would prefer to only model on the state level, there is still a strong argument as seen in the Strait of Malacca case study that one can model large transnational corporate actors on the same level as states. Lloyd's of London represents one such actors, and specifically an international insurance actor. Corporate actors most certainly have a stake in large economic nodes and so their decisions and incentive structures within the larger system should not be ignored. Insurance-industry corporate actors play a particularly relevant role when it comes to economic security because if we evaluate the incentives of this specific set of decision makers, we quickly see that they have a great vested interest in evaluating the economic security of a node, or system of nodes, and investing accordingly. Where they show concern by upping insurance costs or otherwise asking for better security in an area or class of assets, there is with good probability a very real threat to economic security worthy of further investigation by state actors. Understanding these incentives towards action when it comes to corporate actors can then logically be very informative to state actors who wish to maintain effective economic security.

If we use the economic risk framework at a more granular level to evaluate the risk towards these nodes, the difference between the threat of terrorism to the conduit and the threat of increased insurance cost becomes even more defined. Evaluating the risk of a terrorist attack in the strait, we see that the likelihood was quite low and arguably decreasing as discussed in the case study. Looking at the component of severity, it can be seen that the potential damage in terms of assets in particular investor fear could be much more severe. In putting these components together we find the risk to be comparable to other severe but unlikely events. Comparing this to the threat of increased insurance premiums, we know that in suggesting increased rates, the Joint War Committee of Lloyd's of London was ensuring that such rate increases were quite likely if not close to certain, and indeed in the following months the increases did occur. Looking to the severity of this threat, the economic cost was no light matter as 0.1 % of the hull or cargo value of these ships ran into the millions. Though perhaps not comparable to a large terrorist attack, the psychological effects of such a declaration as one that claimed the Strait as unsafe was not insignificant to investors either. Putting the components of likelihood and severity together to evaluate the risk represented by the JWC's declaration on security in regard to the Strait of Malacca, a high likelihood combined with a high severity, though perhaps not as high as the severity of a large scale terrorist attack, still rates the JWC's threat as a greater risk than that of a terrorist attack. Combining this with what is understood about the stakeholder actors in the economic system, as well the structure of the nodes in the system itself, it follows that they would respond more to the threat of increased insurance costs for maritime commerce over the less material and likely threat of terrorism in and of itself. The littoral states are naturally sensitive to trends in maritime commerce, and so they must work with powerful maritime shipping and commerce associations of a corporate nature, who for their part are highly sensitive in turn to any costs of business that might affect their economies of scale. Increased insurance premiums affecting the industry widely and severely as with those that did in the case study most certainly threated profit margins for business in the area. The problem of these business actors quickly became the problem of their governments and so it came to the littoral states to take security actions so as to secure the strait and appease Lloyd's. Having done so eventually, Lloyd's, whose incentive was to preserve their own profit margins by reducing the threats to economic security in the Strait of Malacca, was then willing to have the rates lowered and in doing so the economic damage on part of the local economies was averted in the long term.

5 A Discussion of Safeguards

Most security models identify risks and their nature so that safeguards that mitigate said risks can be introduced and managed. As seen in the case study and many other historical scenarios, when it comes to international economic security, traditional conceptions of safeguards and their use can be problematic. If we think of the most basic safeguard in concept to be something like a wall, we quickly see why this conflicts with the idea of commerce and the profits that an analyst in the field of economic security will be trying to protect. If all conduits to a node are shut down, then although it is true that no threats can access the node through those conduits and damage it, that economic node's ability to accomplish its basic goal of production and profit will be reduced, especially in the age of globalization where competitiveness comes from economies of scale and international trade. When the trade towers fell, the United States response of increasing border security and in particular air transportation security is well known to have had negative economic consequences. The discussion on safeguard in the realm of economic security then must be centered on a balance between security and openness, the willingness to allow risk in parallel to how companies must take risk (speculative risk as described previously) to profit. In particular, the challenge of economic security may well be to effectively address pure risk without impeding the speculative risk that is needed for economic nodes and enterprises to prosper.

In the case study, local business and state actors representing the littoral states were no doubt reluctant to accept the United States' narrative of increased security to fight terrorism in the area because they presumed that such actions, though intended to safeguard, would threaten the economy (not to mention the sovereignty) of the area more than the terrorist attacks in and of themselves. Thus it can be said that the proposed safeguards in that case were seen as impediments to the economic security of the area, rather than effective safeguards for the purpose of economic security. Meanwhile, investors persisted in a state of acceptance for the safeguard of insurance which is more sensitive to the challenges of economic security and certainly less heavy handed. So great was the acceptance of this safeguard that banks required, rather than encouraged or suggested, shipping enterprises to be insured before they could receive loans or investments at all. When the threats to economic security in the Strait of Malacca were framed from an insurance perspective, and motivated by insurance levers, the response on the state and business level was then much more notable because insurance safeguards were so much more fundamental to the system. Ultimately, this sort of sensitivity to the needs of economic systems, their nodes, conduits, and stakeholder actors is what is required to create effective safeguards in respect to economic security.

References

Branch D, Wood EJ (2010) Revisiting counterinsurgency. Politics Soc 38(1):3–14

Control Global (2014) The rocky relationship between safety and security. Retrieved from http://www.controlglobal.com/whitepapers/2014/rocky-relationship-between-safety-and-security/

Deutch J, Schlesinger JR, Victor DG (2006) National security consequences of US oil dependency. COUNCIL ON FOREIGN RELATIONS NEW YORK

Greenhill KM, Staniland P (2007) Ten ways to lose at counterinsurgency. Civil Wars 9(4): 402–419

Knight RF, Pretty DJ (1996) The impact of catastrophes on shareholder value. Templeton College

Lewis TG (2014) Critical infrastructure protection in homeland security: defending a networked nation. Wiley, London

Lobo-Guerrero L (2010) Insuring security: biopolitics, security and risk. Routledge, London

Lobo-Guerrero L (2012a) Insuring war: sovereignty, security and risk. Routledge, London

Lobo-Guerrero L (2012b) Lloyd's and the Moral Economy of Insuring Against Piracy: Towards a politicisation of marine war risks insurance. J Cult Econ 5(1):67–83

McDougall A, Radvanovsky R (2008) Transportation systems security. CRC Press, Boca Raton, FL

Pierides D (2014) Political economies of security for some time to come. J Cult Econ 7(3): 371–377

Qu X, Meng Q (2012) The economic importance of the Straits of Malacca and Singapore: an extreme-scenario analysis. Transp Res Part E: Logistics Transp Rev 48(1):258–265

Reinhart CM, Rogoff K (2009) This time is different: eight centuries of financial folly. Princeton University Press, Princeton, NJ

Rodrigue JP (2004) Straits, passages and chokepoints: a maritime geostrategy of petroleum distribution. Cahiers de géographie du Quebec 48(135):357–374

Shelley L (2004) Unholy trinity: transnational crime, corruption, and terrorism, The. Brown J World Aff 11:101

Weitz GR (2008) Lloyd's of London as a transnational actor: Maritime security cooperation in the Malacca Straits since 9/11. Fletcher School of law and Diplomacy (Tufts University)

Werb D, Rowell G, Guyatt G, Kerr T, Montaner J, Wood E (2011) Effect of drug law enforcement on drug market violence: A systematic review. Int J Drug Policy 22(2):87–94

Critical Infrastructure Vulnerabilities: Embracing a Network Mindset

Tie Xu and Anthony J. Masys

Abstract Critical Infrastructure has become fundamental to the functioning of our society. With the increasing interdependencies within critical infrastructure, the failure or damage of electric power grid, transportation networks, telecommunications, healthcare and water-supply systems would not only cause huge social disruption but also have significant national security implications that can cascade across borders. Developing effective protection, mitigation and recovery measures for critical infrastructures is paramount in the wake of increasing natural and human-initiated hazards, risks and threats. In the past decade, unprecedented technological advancements, rapid institutional changes and trans-boundary dependencies have changed the landscape of infrastructure systems. Critical infrastructure has now evolved into highly interconnected and interdependent networks of socio-technical systems in which different technological layers are interoperating crossing borders within the environmental, social and organizational context that drive their design, operations and development (Masys in Networks and network analysis for defence and security. Springer Publishing, 2014a, b). Understanding the nature of system interdependencies and emerging vulnerabilities can play an essential role in managing and/or reducing the probabilities and consequences of cascading failures in interdependent systems. In this light, the overall objective of this chapter is to address the knowledge gap existing in the dominant risk and disaster management theories by challenging and improving our networked mental model in order to better understand the interdependency-induced vulnerability pertaining to critical infrastructures thereby developing effective protection measures and enabling organizational resilience (Masys in Innovative thinking in risk, crisis and disaster management. Gower Publishing, UK, 2012a, Int J Disaster

T. Xu (✉)
University of Modern Sciences, Dubai, United Arab Emirates
e-mail: t.xu@ums.ae

A.J. Masys
University of Leicester, Leicester, UK
e-mail: anthony.masys@gmail.com

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_9

Prev Manage 21(3):320–335, 2012b). For policy makers, infrastructure owners/operators and researchers as target audience, this chapter will identify emerging challenges to the traditional security thinking in this field and suggest alternative approaches to risk assessment, vulnerability analysis.

Keywords Critical infrastructure · Systems · Vulnerability · Networks

1 Introduction: Concept and Definitions

Today there exists a growing dependence on the continuous flow of essential goods and services provided by infrastructure systems such as energy (electricity, oil and gas supply), information and telecommunication, transportation (by road, rail, air and sea) and water supply including waste water treatment (Gheorghe et al. 2006). Kroger and Zio (2011: 1) regard these critical infrastructure '…so vital to any country that their incapacity or destruction would have a debilitating impact on the health, safety, security, economics, and social well-being'. A failure within one of these infrastructure systems or the loss of its continuous service may be damaging enough to a society and its economy, while that which cascades across boundaries has the potential for multi-infrastructural collapse and unprecedented consequences yielding significant security concerns. Critical infrastructures (CIs), as suggested by Kroger and Zio (2011: 1), are 'various by nature, e.g., physical-engineered, cybernetic or organizational systems, and by environment (geographical, natural) and operational context (political/legal/institutional, economic, etc.)'. Critical infrastructure can be broadly defined as the assets, systems, and networks, whether physical or virtual '[…] so vital and ubiquitous that their incapacity or destruction would not only affect the security and social welfare of any nation, but also cascade across borders' (Gheorghe et al. 2007: 3). Critical infrastructure vulnerability and protection is thereby paramount on the security agenda.

2 Critical Infrastructures Operation: Growing Complexity and Mutual Dependence

In recent decades critical infrastructure systems have grown into a large-scale array of interconnected networks, Fig. 1, with much greater and tighter integration and interdependence. To a large degree CI are mostly privately owned and/or operated and function collaboratively and synergistically to produce and/or distribute a continuous flow of goods and services (Kroger 2010: 1).

Market changes (regulation and deregulation), policies, politics and owners/operators mindset (goals and focus) have shaped the evolution of CI. As described

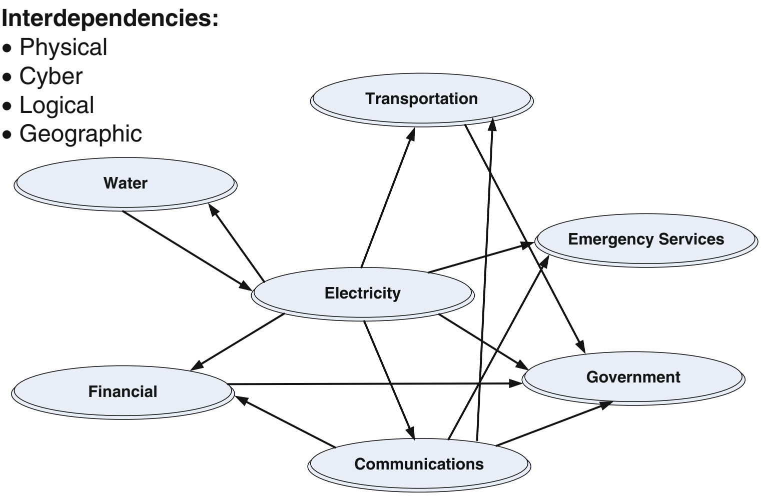


Fig. 1 Interactions among critical infrastructures

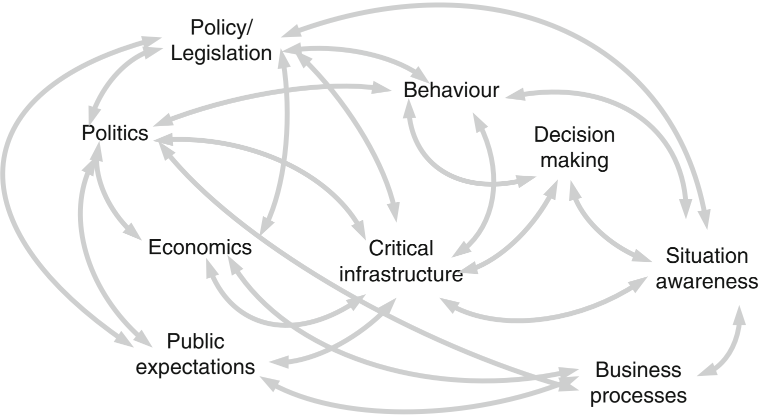


Fig. 2 Complex interactions amongst critical infrastructures (Masys 2014a)

in IRGC (2006), this has resulted in improved service and convenience but also has increased social vulnerabilities in the face of accidental or intentional disruption. CI and its inherent vulnerabilities (captured by the hyper/hybrid risks (Helbing 2013; Masys et al. 2014) has been shaped by this socio-technical-political-economic-ecological influences (Fig. 2).

Rinaldi et al. (2001: 11) argues that 'The notion that our nation's critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies is more than a theoretical concept'. Rapid institutional changes (i.e., shifting from public to private entities, deregulation, privatization, market-driven economies, etc.) and technological changes have changed the landscape of critical infrastructure systems (Calida and Katina 2012). As described in the IRGC (2006: 12) report, the factors which have contributed to a hyper connectivity, interdependency and vulnerability lie amongst factors such as:

- ‘Incremental and erratic integration of smaller systems into larger systems, thus creating greater complexity and enabling the trans-boundary propagation of disturbances
- Changes in the economic, environmental, legal, and regulatory settings in which the systems operate, including economic pressures which have reduced operating margins and, thus, squeezed out slack or redundancy in systems
- Growing complexity of new and existing systems (facilitated by more capable ICT)
- Use of off-the-shelf technology, including information and control systems, motivated by short-term economic efficiency
- Lack of adequate awareness of vulnerabilities, of the limitations to achievable reliability, or of concern for low-probability but high-consequence failure modes’ (IRGC 2006: 12).

Interactive complexity (Perrow 1984) characterizes critical infrastructures operating within a dynamic environment. Risk formulations related to critical infrastructures must consider factors beyond those commonly associated with risk. Specifically, risk formulation in this field requires the consideration of how infrastructures operate with respect to their interconnected and trans-boundary effects (Katina and Pinto 2012) and in particular leveraging the socio-technical perspective. As described in Masys (2014a: 267) vulnerability analysis of CI requires that we ask such questions as:

- How do we define the boundaries of the system
- What are the relevant threats and hazards associated with the system (an examination of the space of possibilities)
- How is resilience realized within the system
- How do the interdependencies shape the structure and dynamics of the system
- What are the uncertainties
- Do resident pathogens [such as normalization of deviance (Vaughan 1996)] exist.

The vulnerability of all of these infrastructures arises from the complex interdependencies, such that the state of a system depends on the state of other systems (Gheorghe et al. 2007) which includes the state of the social and organizational that characterize the socio-technical domain (Masys 2012a, b, 2014a, b). The electricity and communication networks are particularly vital for the smooth functioning of other infrastructures. Kroger and Zio (2011: 5) define vulnerability as ‘[…] a flaw or weakness in the design, implementation, operation, and/or management of an infrastructure system, or its elements, that renders it susceptible to destruction or incapacitation when exposed to a hazard or threat, or reduces its capacity to resume new stable conditions'. Risk Governance Council (IRGC 2006) suggests that infrastructure vulnerability is an important area of research, especially with regards to coupled infrastructures because it can lead to the discovery of emerging weaknesses in the infrastructures due to mutual interdependence.

Beck (1992, 2009) risk society describes how risks arise and spread through highly connected networks. Such connectivity makes modern social-technical systems highly complex, unpredictable and often vulnerable to social, natural and technical hazards. Recent disasters such as Hurricane Katrina in 2005 and Hurricane Sandy in 2012 highlight the vulnerability of critical infrastructure to conjoint events of social, natural and technical disasters. The linear agent-consequence analysis is no longer valid in this highly interconnected world where risks migrate and evolve (Masys 2012a, b, 2014a, b). As such our understanding of their complex aetiology and management must be considered from a '**networked mental model**' that recognizes the interdependency-induced vulnerability embedded in the complex structures, processes and dynamics of modern social-technical systems (Vespignani 2009). However, currently there is a dearth of understanding regarding security, vulnerabilities and the nature of system interdependences in critical infrastructures as it pertains to hyper/hybrid risks and their implications on the security agenda (Masys et al. 2014).

3 Hyper-critical Infrastructure (Hyper/Hybrid Risks)

The electricity supply systems and information and telecommunication systems are particularly vital for the smooth functioning of other critical infrastructures (IRGC 2006: 12). As such the hyper/hybrid risks (Helbing 2013; Masys et al. 2014) that reside and permeate the CI domain is relevant to the energy and ICT sectors.

Electricity supply, generation, transmission, distribution and consumption is the lifeblood of society. Vulnerabilities to this stemming from hyper risks make energy security a top priority for national security. The degree of criticality is high as the impact of a failure, loss or unavailability can be significant in scope with immediate effect both nationally and cross-border (IRGC 2006; Masys 2014a, b; Johnson 2008; Kroger and Zio 2011). Johnson (2008) describes the devastating affect of the power outage on 28th September 2003 across Italy and Switzerland:

> The immediate trigger was a fault in the Swiss transmission system. The consequences propagated across international borders affecting the networks in France, Slovenia, and Austria. It also led to a domino effect that ultimately led to the separation of the Italian system from the rest of the European grid.
>
> - More than 56 million people lost power across Italy and areas of Switzerland.
> - Rolling blackouts were used to prevent demand from exceeding supply during this restoration phase.
> - 30,000 people were trapped on trains.
> - Several hundred passengers were stranded on underground transit systems.

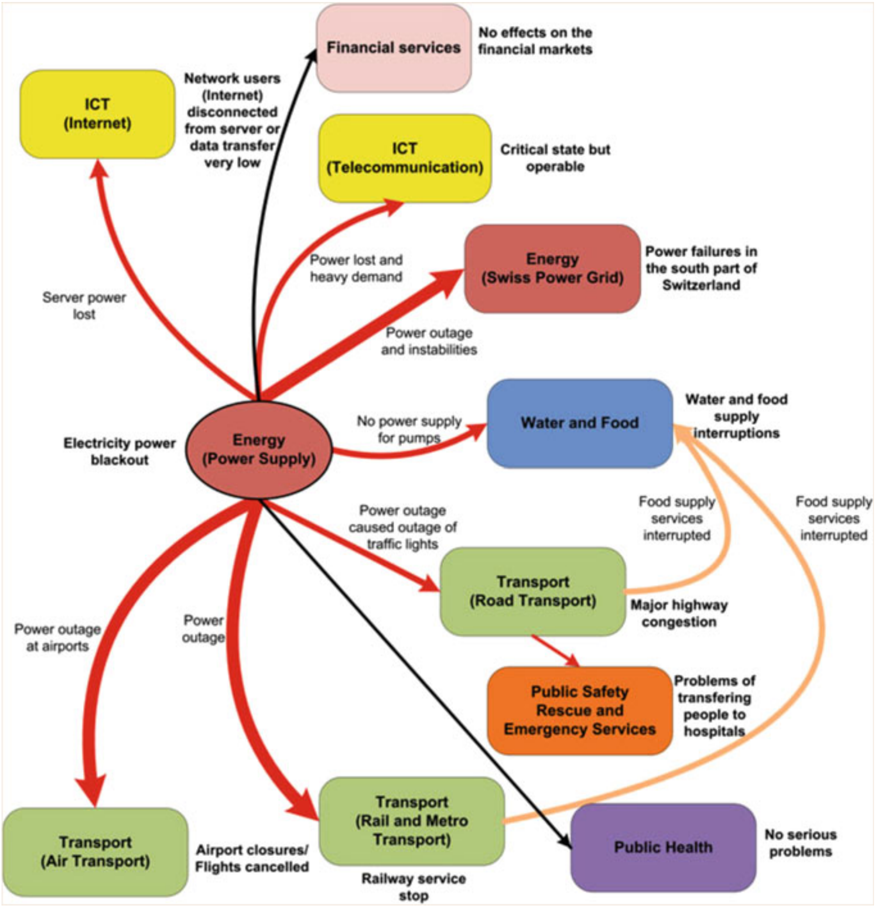

Financial services
No effects on the financial markets
ICT (Internet)
Network users (Internet) disconnected from server or data transfer very low
ICT (Telecommunication)
Critical state but operable
Energy (Swiss Power Grid)
Power failures in the south part of Switzerland
Power lost and heavy demand
Server power lost
Power outage and instabilities
Water and Food
Water and food supply interruptions
No power supply for pumps
Electricity power blackout
Energy (Power Supply)
Food supply services interrupted
Food supply services interrupted
Power outage caused outage of traffic lights
Transport (Road Transport)
Major highway congestion
Public Safety Rescue and Emergency Services
Problems of transfering people to hospitals
Power outage at airports
Power outage
Transport (Air Transport)
Airport closures/ Flights cancelled
Transport (Rail and Metro Transport)
Railway service stop
Public Health
No serious problems

Fig. 3 The impact of the Italian blackout 2003 on other infrastructure sectors (Kroger and Zio 2011: 13)

- Although hospitals and other emergency centres were able to call upon reserve generators, there were significant knockon effects across other critical infrastructures.
- The mobile phone system began to fail as transceivers lost power.
- Other areas of the networks became overloaded as customers tried to contact friends and family. The blackout also affected large areas of the Internet as UPS sources either failed or ran out of battery power.

Johnson (2008) describes a complex aetiology that reified as the failure of technical vulnerabilities that, in turn, stemmed from changes in the regulation and monitoring of energy transfers across Europe as well as managerial and human factors causes (an over-reliance on computer-based decision support systems). Similarly, Kroger and Zio (2011) examining the dimensions of interdependency and vulnerability (Fig. 3) and the requirement to think beyond piecemeal back-ups but to think with a more ‘networked mindset’.

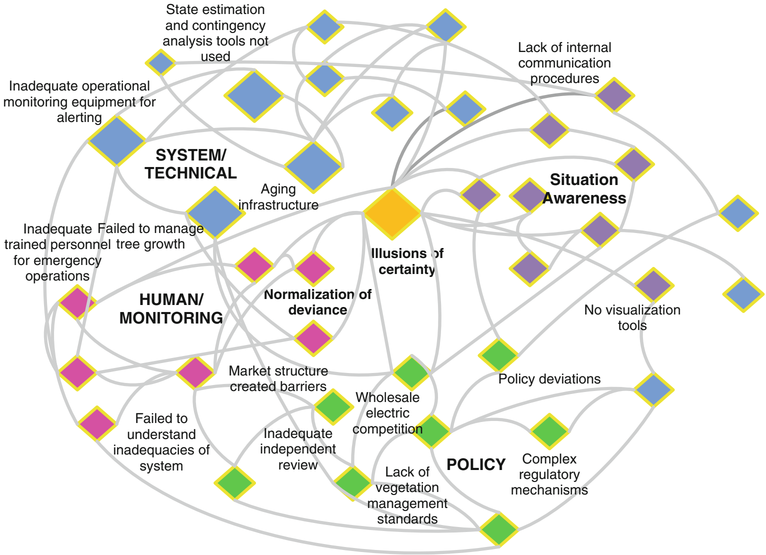

State estimation and contingency analysis tools not used
Inadequate operational monitoring equipment for alerting
SYSTEM/ TECHNICAL
Aging infrastructure
Lack of internal communication procedures
Situation Awareness
Inadequate trained personnel for emergency operations
Failed to manage tree growth
Illusions of certainty
HUMAN/ MONITORING
Normalization of deviance
No visualization tools
Market structure created barriers
Policy deviations
Wholesale electric competition
Failed to understand inadequacies of system
Inadequate independent review
POLICY
Complex regulatory mechanisms
Lack of vegetation management standards

Fig. 4 Actor network representation of 2003 US/Canada Blackout (Masys 2014a)

Like the Italian blackout, the 2003 Blackout in US/Canada described in Masys (2014a) captures the hyper-risks that characterize the event. Shaped by socio-political-technical-economic-ecological factors, the hyper-risks emerged as resident pathogens in the system (Fig. 4). For example as described in IRGC (2006: 19), '…vulnerabilities that could lead to service disruption or quality degradation are introduced via perfectly innocent procurement choices to use off-the-shelf commercial systems'.

Both cases show how vulnerabilities within CI can be seeded into the system. Triggering the vulnerabilities can result in a cascading event that can significantly affect societal operations and have national security implications that are cross domain. For example concerning water and health security, the US/Canada blackout '…shut down all major pumping stations which serve more than 1 million residents…in Detroit five days after the outage tap water was still undrinkable. In major cities (e.g. New York) streams of raw sewage began to flow into surrounding waterways posing health and environmental hazards' (IRGC 2006: 37).

4 Emerging Systemic Risks to Critical Infrastructure Protection

Emerging system-related risks driven by the growing complexity and interdependence of systems (IRGC 2010) is of particular concern to critical infrastructure protection. The erosion of safety or 'drift to failure' (Dekker 2011) stems from the pace at which many of these systems operate, often under higher levels of stress as well as the high levels of connectivity and interdependence. Legacy systems become embedded in the opaque ‘system of system’ within which lie resident pathogens stemming from misaligned policies, procedures and hard-wired politics (Masys 2010, 2012a, b).

5 CI Interdependence and Vulnerability Analysis

While some interdependent and coupling behavior between infrastructures has always existed, today, the criticality emerges from the hyperconnectivity across CI where impact has local, regional and cross border implications. Risk formulation in such interconnected “system of systems” should consider the bidirectional nature of relationships as well as 2nd, 3rd, and 4th order effects (downstream dependencies) among critical infrastructures. As such, risk formulation for a critical infrastructure would include: (i) the probability of occurrence of an event; (ii) the consequence of occurrence of the event; and (iii) the interdependency factor that accounts for the external relationship beyond the infrastructure of interest (Katina et al. 2014: 16). The research literature indicates that risk formulation in the field of critical infrastructures requires a better understanding of the interdependencies existing between infrastructures (Katina and Hester 2013). Currently there is a paucity of such understanding that captures the nature of system interdependences in critical infrastructures, which must operate as integrated wholes in the wake of increasingly ‘unpredictable’ landscape of hazards, risks and threats.

6 Enhancing Security Through Understanding Infrastructure Interdependencies

The contemporary vulnerability of critical infrastructures derives essentially from the intricate, often nonlinear interactions among a large number of interconnected and geographically distributed components of different types, including both technical and non-technical elements. Even their interaction with the regulatory, legal or institutional framework may eventually affect the overall vulnerability of infrastructure systems (Kroger and Zio 2011; Masys 2012a, b, 2014a). Furthermore, the normal operation of these systems does not allow for the detection of hidden interactions across CI domains which might become crucial for the evolution of cascading failure events. The dynamic degradation of networks and the systemic behavior cannot be described and explained by linear equations. When examining the case of multiple infrastructures connected as a “system of systems,” we must consider interdependencies (Rinaldi et al. 2001). Rinaldi et al. (2001: 14) define infrastructure interdependency as ‘…A bidirectional relationship between two

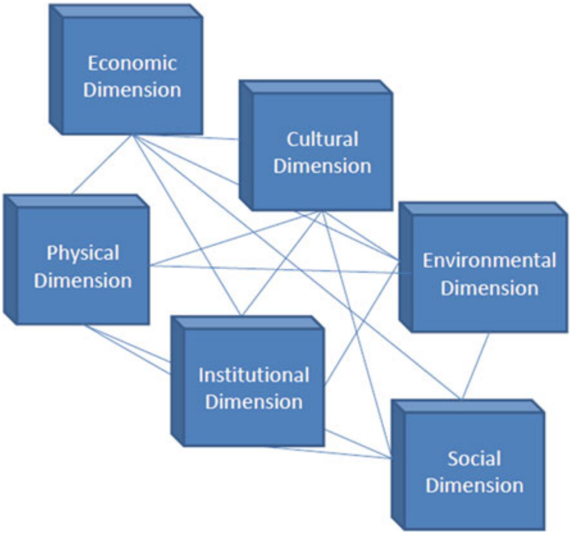


Fig. 5 Examples of critical infrastructure vulnerability interdependencies

infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other'.

The recognition that infrastructures do not operate in isolation suggests the need to develop infrastructure protection measures (i.e., detection, mitigation and recovery) that capture the intricate relationships existing between infrastructures. Given the complexity associated with todays socio-technical systems (Critical Infrastructure), vulnerability thereby emerges as multidimensional. As described in Birkmann et al. (2013: 200–201) six characteristic vulnerabilities emerge (Fig. 5):

- **Social dimension**: propensity for human well-being to be damaged by disruption to individual (mental and physical health) and collective (health, education services, etc.) social systems and their characteristics (e.g. gender, marginalization of social groups).
- **Economic dimension**: propensity for loss of economic value from damage to physical assets and/or disruption of productive capacity.
- **Physical dimension**: potential for damage to physical assets including built-up areas, infrastructure and open spaces.
- **Cultural dimension**: potential for damage to intangible values including meanings placed on artefacts, customs, habitual practices and natural or urban landscapes.
- **Environmental dimension**: potential for damage to all ecological and bio-physical systems and their different functions. This includes particular ecosystem functions and environmental services but excludes cultural values that might be attributed.
- **Institutional vulnerability**: potential for damage to governance systems, organizational form and function as well as guiding formal/legal and

informal/customary rules—any of which may be forced to change the following weaknesses exposed by disaster and response.

The majority of assets and systems exposed to hazard will exhibit more than one dimension of vulnerability.

As part of a process to identify hazards, risk and multidimensional vulnerabilities that impact the performance of interdependent systems, research literature suggests examining different types of interdependencies for critical infrastructures. These descriptions could be used to articulate the types of interdependencies in risk formulations with respect to the interdependence variable. Rinaldi et al. (2001) categorizes infrastructure interdependencies as physical, cyber, geographical and logical interdependencies. The categorization was extended to include societal and policy ramifications via mathematical formalizations proposed by Dudenhoeffer et al. (2006). Table 1 uses these interdependencies to clarify the relationships existing among interdependent infrastructures with respect to risk implications.

7 Interdependency-Induced CI Vulnerabilities

The inherent complexity in modern social-technical systems challenges our understanding pertaining to their structure, processes and dynamics and thereby our understanding regarding the vulnerabilities and disaster risk reduction of critical infrastructure. The interdependency and interconnectivity that characterizes the CI domain makes it highly complex. Vespignani (2010: 984) argues that '…relatively localized damage in one system may lead to failure in another, triggering a disruptive avalanche of cascading and escalating failures. Understanding the fragility induced by multiple interdependencies is one of the major challenges in the design of resilient infrastructures'. Ray-Bennett et al. (2015) argue that current crisis and disaster theories and practices '…fail to capture the complexities of modern social-technical systems and that of the organizations involved in disaster risk reduction practices'. Most importantly there is a lack of network-oriented understanding of vulnerability embedded in the complex structure, processes and dynamics pertaining to critical infrastructure. Failures in such understanding of vulnerability and foresight informed action are resident within cases such as Hurricane Katrina in 2005 and Fukushima in 2011 as described in Masys (2012a, b) and Masys et al. (2014).

Hurricane Katrina in 2005 devastated New Orleans and is regarded as the most catastrophic natural disaster in American history (Comfort 2006). Focusing on the initiating event that precipitated the infrastructure failure does not capture the root vulnerabilities that are hardwired into the greater networked system. A report by the American Society of Civil Engineers argues that the breach of floodwalls and much of the destruction of New Orleans was not caused by the hurricane itself. It was the result of '[…] a combination of inappropriate decisions and institutional settings

Table 1 Types of interdependencies in critical infrastructures (Katina et al. 2014)

Physical interdependency	Rinaldi et al. state that it "arises from the physical linkage between the inputs and outputs of two agents [where the] commodity produced or modified by one infrastructure (an output) is required by another infrastructure for it to operate (an input)" (e.g., drinking water and electricity)	Risks in one infrastructure directly influence operations (i.e., outputs, product, goods and services) of physical interdependent systems. For example, the availability of clean drinking water physically depends on electrical systems that must purify water. The operator of a water treatment system is concerned with the risks in the electricity system
Cyber interdependency	Related to risks associated with the omnipresence of information and communications technologies. Rinaldi states that "computerization and automation of modern infrastructures and the widespread use of SCADA systems have led to pervasive cyber interdependencies"	Management must consider the risks associated with outputs, products, goods and services that depend on information and communications systems (e.g., SCADA systems). The use of data and information provides connections to other systems that might not exist
Geographical interdependency	DiSera and Brooks (2009) state that a geographical interdependency exists when different infrastructure systems share the same environment (e.g., power lines share the same corridor with a bridge)	A common environment is needed for coupling infrastructure systems and their components. However, this poses a threat to all infrastructures in the same corridor (e.g., an explosion threat to a bridge affects the bridge and power lines)
Logical interdependency	Infrastructure systems can have logical interdependencies if the state of one infrastructure depends on the state of another infrastructure via a mechanism that is neither physical, cyber nor geographical. An example is the linkage between the 1996 power deregulation policy and the energy crisis in California in the 2000s	Interconnections between infrastructures must be analyzed beyond time and space with respect to physical, cyber and geographic mechanisms. For example, the consideration of policy and its possible influence on operations regardless of space or time between infrastructures and the point of origin
Policy and/or procedural interdependency	Interdependence becomes apparent only after changes take place so that the functioning of one infrastructure is impacted by changes in policies/procedures in another infrastructure (e.g., after the 9/11 attacks, U.S. Congress issued regulations affecting all air transportation systems (Mendonca and Wallace 2006)	It is necessary to analyze how changes in national, state, regional and local policies influence infrastructure operations, including the quality of goods and services across time and space

(continued)

Table 1 (continued)

Societal interdependency	Dudenhoeffer et al. (2006) state that societal interdependencies arise when infrastructure operations are affected by public opinion (e.g., after the 9/11 attacks, air traffic was reduced due to the public's evaluation of travel safety, resulting in job cuts and bankruptcies)	It is necessary to analyze the actions of the public and relate the actions to popular opinion regarding critical infrastructure operations. The results may be used to inform understanding about the possible influence on goods and services that the infrastructure of interest provides to the public

made over the years […] reflecting a lack of foresight and a thinking paradigm that did not consider the inherent vulnerabilities embedded in the complex network of infrastructure systems' (ASCE 2007; cited in Masys 2012a, b: 327). Similarly, this lack of isomorphic foresight and a networked mental model resonates with Fukushima in 2011 whereby an earthquake and resulting tsunami had a devastating effect on the Fukushima Diiachi nuclear power plant. This vulnerability described in IAEA (2015) identifies the lack of 'assumption challenge' as a key factor in the accident aetiology. Assumption Based Planning (ABP) (Dewar et al. 1993) is an excellent approach that provides insights into how in the Fukushima disaster there was failure in the process model to articulate, verify and validate assumptions. ABP lends itself to examine the volatility and instability of assumptions that are seeded into socio-technical design and operations. The DIET Report Executive summary (2013: 9) argues that although the earthquake and tsunami of March 11 2011 are considered triggers of the cataclysmic event, 'the subsequent accident at the Fukushima Daiichi Nuclear Power Plant cannot be regarded as a natural disaster. It was a profoundly manmade disaster'.

Described in Masys et al. (2014), the failure of imagination is a stark reminder of the findings of The 9/11 Commission Report (2004: 336) that articulated '…a failure of imagination and a mindset that dismissed possibilities' as a key underlying factor. Mindset is not a new concept as it pertains to disasters. The Three Mile Island accident investigation also pointed out that a mental model '…in which an insufficient consideration of the human element had converted minor equipment malfunctions into a severe accident' (Walker 2004: 211). Similarly, the Lac-Mégantic rail disaster in 2014 highlights mental models that contributed to a poor safety culture. The TBS report (2014) highlights:

> An organization with a strong safety culture is generally proactive when it comes to addressing safety issues. MMA was generally reactive. There were also significant gaps between the company's operating instructions and how work was done day to day. This and other signs in MMA's operations were indicative of a weak safety culture—one that contributed to the continuation of unsafe conditions and unsafe practices, and significantly compromised the company's ability to manage risk.

Current mental models derived from the dominant crisis and disaster theories and practices reveal their inadequacies to address the complex, nonlinear and dynamic interconnectivity and interdependence that exists in modern social-technical systems.

In this way, as illustrated by Hurricane Katrina in 2005 and Fukushima in 2011, such mental models can cause fateful decisions and the repetition of previous mistakes. This calls for a paradigm shift in disaster risk reduction thinking: 'systemic instabilities can be understood by a change in perspective from a component-oriented to an interaction- and network-oriented view' (Helbing 2013: 51). Therefore, it is argued that events of socio-technical failure can be understood only by analyzing its paradigm of interdependency, complexity and wholeness. A new disaster risk reduction paradigm is required to support the networked understanding of vulnerability as it pertains to critical infrastructure; one that will develop not only anticipatory measures for risk management but also prepare for the unpredictable and the unknown by building organizational resilience (Helbing 2013; Ray-Bennett et al. 2015).

8 Systems Thinking

Systems thinking, according to Senge (1990), is a theoretical perspective for seeing interrelationships rather than entities in isolation, for seeing patterns of change rather than static snapshots. As a worldview, systems thinking recognizes that socio–technical systems cannot be addressed through a reductionist approach that reduces the systems to their components. The behavior of the system is a result of the interaction and interrelationships that exist, thereby acknowledging emergent behaviors and unintended consequences. It is through understanding such a paradigm that we can develop the complex disaster aetiology and isomorphic lessons. As a disaster management discipline, systems thinking helps us to see the structures and deeper patterns that underlie complex situations thereby challenging simplification and opening our mental models up to a space of possibilities (Jackson 2003: 65). Following a systems thinking perspective there are a range of conceptual tools in the literature that can support network-oriented vulnerability analysis for building 'active foresight' as it pertains to disaster risk reduction (Van der Merwe 2008). The works of Trist (1981) socio-technical systems; Kauffman (1995) complexity; Prigogine (1989) instability; Beer (1995) cybernetics; Jackson (2003) critical systems approach; Checkland (2001) soft systems methodology; Ackoff (1999) Action Research; Senge (1990) systems thinking; Sterman (2000) systems dynamics figure prominently. Among these conceptual tools and approaches, scenario planning is viewed as an important application of systems thinking for isomorphic foresight that support reflective practices to enable a change in the mindset of the people who uses it (Masys 2012a, b, 2014; Farber and Lakhtakia 2009: S13).

The features of systems thinking that shape the analysis of the CI stem from the conceptualization that the general system is not simply an aggregation of objects but is rather a set of interrelated, interconnecting parts. Ottino (2003: 293) argues that 'complex systems cannot be understood by studying parts in isolation. The very essence of the system lies in the interaction between parts and the overall behaviour that emerges from the interactions'. The systems perspective of actor network theory (ANT) examines the socio-technical system and looks at the inter-connectedness of the heterogeneous elements characterized by the technological and non-technological (human, social, organizational) elements (Masys 2010, 2012a, b). The network space of the actor network provides the domain of analysis that examines the critical infrastructure as a network of heterogeneous elements to reveal the inherent vulnerabilities. Yeung (2002) notes that much of the work that draws on actor network theory places its analytical focus on unearthing the complex web of relations between humans and non-humans.

With respect to critical infrastructure, Vespignani (2009: 428) describes how '… in power grids and other flow-carrying networks, the failure of a single node or line can trigger a domino effect (cascading failure) in which the overload induced by the flow redistribution may generate a global failure of the network'. Network thinking, as described in Barabasi (2003) opens novel perspectives to understanding complex systems such as markets and economic system, socio-technical systems, criminal and terrorist networks. This network thinking mindset leverages a topological analysis which is based upon classical graph theory through which interesting properties of the structure of a network system can be revealed. The properties of interdependency and interconnectivity resident within these networks can also be examined from a temporal perspective thereby revealing interesting dynamic properties of an evolving network. Such analysis can be instrumental in assessing vulnerabilities of critical infrastructures that can shape operating and design decisions.

Analysis through a socio-technical system thinking lens (Masys 2010, 2012a, b), recognizes the entangled state space described by these systems which can be conceptualized as the hybrid collectif (Callon and Law 1995; Masys 2010, 2012a, b), the intersection of the physical, human and informational domains (Fig. 6).

An examination of actors such as those characterized from technologies to policies and the relations inherent within the actor network (Masys 2012a, b), facilitates an exploration of how these "actors" mediate action and how they are entangled in local socio-technical/political configurations. The lens of ANT facilitates the view of the world in terms of heterogeneous elements, thereby employing a "systems thinking" perspective of the problem space.

The Nonlinear interactions that transcend physical, spatial and temporal domains characterize the actor network analysis. Vulnerability analysis reveals a complex,

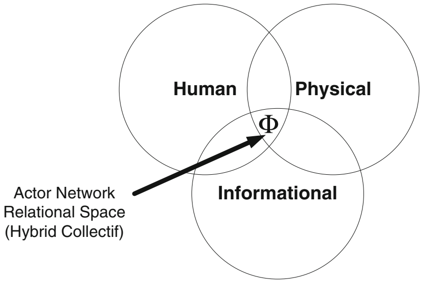


Fig. 6 Hybrid collectif (Masys 2010)

coupled network thereby suggesting that design and operation of such systems requires a requisite complex perspective to understand structure and dynamics. Systems thinking and network thinking become key enablers in CI management. Helbing (2013: 53) argues that '…Individual risks may rightly have been viewed as small, but the risk to the system as a whole was vast'. Coping with networked 'hyper-risks' requires a humble recognition of the complexity of CI systems. ANT explores the ways that the networks of relations are composed, how they emerge and come into being, how they are constructed and maintained, how they compete with other networks, and how they are made more durable over time. It examines how actors enlist other actors into their world and how they bestow qualities, desires, visions and motivations on these actors (Latour 1996).

9 Conclusions

For policy makers, infrastructure owners/operators and CIP researchers as target audience, the authors derived some informative understanding on the risks and security challenges facing critical infrastructures and the emerging vulnerabilities associated the increasing interdependence between them as a highly complex 'system of systems'. Today, critical infrastructures are highly complex and interconnected social-technical systems. Their interdependencies and coupling behaviors are challenging our abilities to understand the inherent vulnerabilities that lie within and thereby becoming a key element in the national security agenda. We determine vulnerability be examining the hyper/hybrid risks that permeate the complex problem space. Network mapping (Fig. 5) shows the high level interdependencies and hence qualities of exposure, fragility, resilience and adaptive capacities that exist across the heterogeneous actors of critical infrastructure (Masys 2012a, b, 2014a, b).

References

Ackoff RL (1999) On passing through 80. Syst Pract Action Res 12(4):425–430

ASCE (2007) The New Orleans hurricane protection system: what went wrong and why. A report by the ASCE Hurricane Katrina external review panel. ASCE Press, Reston

Barabasi A-L (2003) Linked: the new science of networks. Plume Books, Cambridge

Beck U (1992) Risk society: towards a new modernity. Sage, London

Beck U (2009) What is globalization?. Polity Press, Cambridge

Beer S (1995) Designing freedom. John Wiley, Chichester

Checkland P (2001) Soft systems methodology. In: Rosenhead J, Mingers j (eds) Rational analysis for a problematic world revisited. John Wiley and Sons Ltd., West Sussex

Birkmann J, Cardona OD, Carreno ML, Barbat AH, Pelling M, Schneiderbauer S, Kienberger S, Keiler M, Alexander D, Zeil P, Welle T (2013) Framing vulnerability, risk and societal responses: the MOVE framework. Nat Hazards 67:193–211

Calida B, Katina P (2012) Regional industries as critical infrastructures: a tale of two modern cities. Int J Crit Infrastruct 8(1):74–90

Callon M, Law J (1995) Agency and the hybrid *collectif*. South Atlantic Q 94(2):481–507

Comfort LK (2006) Cities at risk: Hurricane Katrina and the drowning of New Orleans. Urban Aff Rev 41(4):501–516

Dekker S (2011) Drift into failure: from hunting broken components to understanding complex systems. Ashgate, Burlington

Dewar JA, Builder CH, Hix WM, Levin MH (1993) Assumption based planning: a planning tool for very uncertain times. http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR114.pdf

DIET Report Executive Summary (2013) Available online at: http://www.nirs.org/fukushima/naiic_report.pdf. Accessed 20 Oct 2014

DiSera D, Brooks T (2009) The geospatial dimensions of critical infrastructure and emergency response. Pipeline Gas J 236(9):1–4

Dudenhoeffer D, Permann M, Manic M (2006) CIMS: a framework for infrastructure interdependency modeling and analysis. In: Proceedings of the thirty-eighth winter simulation conference, pp 478–485

Farber D, Lakhtakia A (2009) Scenario planning and nanotechnological futures. Eur J Phys 30(4): S3–S15

Gheorghe A, Masera M, Weijnen M, De Vries L (2006) Critical infrastructures at risk: securing the European electric power system, vol 9. Springer, Dordrecht

Gheorghe A, Masera M, De Vries L, Weijnen M, Kroger W (2007) Critical infrastructure: the need for international risk governance. Int J Crit Infrastruct 3(1/2):3–19

Helbing D (2013) Globally networked risks and how to respond. Nature 497:51–59

IAEA (2015) The Fukushima Daiichi accident: report by the director general and technical volumes. https://www.iaea.org/newscenter/news/iaea-releases-director-general%E2%80%99s-report-fukushima-daiichi-accident

International Risk Governance Council (IRGC) (2006) Managing and reducing social vulnerabilities from coupled critical infrastructures. White paper No 3, Geneva, Switzerland. Available at: http://www.irgc.org/IMG/pdf/IRGC_WP_No_3_CriticalInfrastructures.pdf

International Risk Governance Council (IRGC 2010) Assessing and managing emerging risks. Geneva, Switzerland, available at: http://www.irgc.org/IMG/pdf/irgcERfinal07jan_web.pdf

Jackson MC (2003) Systems thinking: creative Holism for managers. Wiley, Chichester

Johnson CW (2008) Understanding failures in international safety infrastructure: a comparison of European and North American power failures. In: Proceedings of the 26th international conference on system safety, Vancouver, BC, 25–29 Aug

Katina P, Pinto C (2012) On critical infrastructure interdependence. In: Presented at the thirty-third national conference of the American society for engineering management

Katina P, Hester P (2013) System determination of infrastructure criticality. Int J Crit Infrastruct 9 (3):211–225

Katina P, Pinto C, Bradley J, Hester P (2014) Interdependency-induced risk with applications to healthcare. Int J Crit Infrastruct Prot 7:12–26

Kauffman S (1995) At home in the Universe: the search for the laws of self organization and complexity. Oxford University Press, London

Kroger W (2010) Emerging risks to large-scale engineered systems, white paper, October 2010. IRGC, Geneva

Kroger W, Zio E (2011) Vulnerable systems. Springer Publishing, Dordrecht

Latour B (1996) On actor-network theory a few clarifications. Soziale Welt 47:369–381

Masys AJ (2010) Opening the black box of human error: revealing the complex aetiology of fratricide. VDM Publishing

Masys AJ (2012a) The emergent nature of risk as a product of 'heterogeneous engineering. A relational analysis of the oil and gas industry safety culture In: S Bennett (ed) Innovative thinking in risk, crisis and disaster management. Gower Publishing, UK

Masys AJ (2012b) Black swans to grey swans—revealing the uncertainty. Int J Disaster Prev Manage 21(3):320–335

Masys AJ (2014a) Critical infrastructure and vulnerability: a relational analysis through actor network theory. In AJ Masys (ed) Networks and network analysis for defence and security. Springer Publishing

Masys AJ (2014b) Dealing with complexity: thinking about networks and the comprehensive approach In: AJ Masys (ed) Networks and network analysis for defense and security. Springer Publishing

Masys AJ, Ray-Bennett N, Shiroshita H, Jackson P (2014) High impact/low frequency extreme events: enabling reflection and resilience in a hyper-connected world. In: 4th international conference on building resilience. Salford Quays, United Kingdom, 8–11 Sept 2014. Procedia Econ Finan 18: 772–779

Mendonca D, Wallace W (2006) Impacts of the 2001 World Trade Center Attack on New York City critical infrastructures. J Infrastruct Syst 12(4):260–270

Ottino J (2003) Complex systems. AIChE J 49(2):292–299

Perrow C (1984) Normal accidents: living with high-risk technologies. Basic Books Inc, New York

Prigogine I (1989) The philosophy of instability. Futures 21(4):396–400

Ray-Bennett N, Masys AJ, Shiroshita H, Jackson P (2015) Reactive to pro-active to reflective disaster responses: introducing critical reflective practices in disaster risk reduction (DRR). In: A Collins et al. (ed) Hazards, risks and disasters in society. Elsevier Publishing, AP

Rinaldi S, Peerenboom J, Kelly T (2001) Identifying, understanding and analyzing critical infrastructure interdependencies. IEEE Control Syst Mag 21(6):11–25

Senge P (1990) The fifth discipline: the art and practice of the learning organization. Doubleday Currency, New York

Sterman JD (2000) Business dynamics: systems thinking and modeling for a complex world. Boston. McGraw-Hill

TBS Report (2014) http://www.tsb.gc.ca/eng/rapports-reports/rail/2013/r13d0054/r13d0054-r-es.asp

The 9/11 Commission Report. 2004. http://www.9-11commission.gov/report/911Report.pdf

Trist E (1981) The evolution of socio-techncial systems. In: Van de Ven H, Joyce WF (eds) Perspectives on organizational design and behavior. John Wiley, New York

Van der Merwe L (2008) Scenario-based strategy in practice: a framework. Adv Dev Hum Resour 10(2):216–239

Vaughan D (1996) Challenger launch decision: risky technology, culture and deviance at NASA. University of Chicago Press, Chicago

Vespignani A (2009) Predicting the behavior of techno-social systems. Science 325 (July): 425–428

Vespignani A (2010) The fragility of interdependency. Nature 464:984–985

Walker JS (2004) Three mile island: a nuclear crisis in historical perspective. The University of California Press, Berkeley

Yeung HWC (2002) Economic geography: old wine in new bottles? Paper presented at the 98th Annual meeting of the Association of American Geographers, Los Angeles, CA. 19–23 Mar 2003. http://courses.nus.edu.sg/course/geoywc/publication/Yeung_AAG.pdf

Supply Chain Information Security: Emerging Challenges in the Telecommunications Industry

Tie Xu and Shereen Nassar

Abstract Given the ramifications of widespread RFID implementation in contemporary supply chain management, there is a need for awareness of emerging security threats and effective self-protection mechanisms against system failures and attacks. The aim of this chapter is to identify the emerging information security challenges pertaining to RFID applications in the telecommunications industry. Having policy makers and telecom operators as the target audience, this chapter will present a conceptual framework for approaching risk management activities in regards to auto-ID/RFID applications with comprehensive and contemporary understanding about information assets, ecosystem threats, and vulnerabilities embedded in their extended supply chains.

Keywords Risk management · RFID · Supply chain · Vulnerability

1 Supply Chain Management and Information Challenge

The prominent force of global supply chain and logistics developments fuelled by globalisation and technological revolution has enabled a worldwide exchange of people, goods, money, information, and ideas (Helbing 2013). In today's highly connected global supply chain networks, organisations are confronted with emerging challenges from a host of internal and external process and information interdependencies. As the complexity of such networked interdependency increases, our global supply chains become increasingly vulnerable to systemic risks, because of which damaging events can spread rapidly and globally. An important aspect of these emergent systemic risks is the result of a complex set of interactions involving explicit and implicit coordinating supply chain communications as well as the transfer of information and physical goods. Expanding on our current

T. Xu (✉) · S. Nassar
University of Modern Sciences, Dubai, United Arab Emirates
e-mail: t.xu@ums.ae

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_10

understanding of systemic risks thus requires looking beyond the vulnerability of individual actors and examining the effect of the consequences of various supply chain information technology disruptions on the ability of the global supply network to produce the required good or service.

1.1 Supply Chain Management Concept

The advancement of Web-enabled communications protocols and the digital economy has revolutionised many aspects of the contemporary supply chain management process. In commerce and industry, firms are now most likely to be connected into networks allowing exchange, access and the ability to leverage information with the potential to significantly improve the management of operations within their organisations and the extended supply chain. The importance of integrating and coordinating organisations in networks to respond to evolving challenges is well acknowledged (Porter 1985; Cooper et al. 1997; Hammer 2001; Lambert 2004). In this context, integrated supply chain management (ISCM) is not only regarded as a dominant factor (Lamming 1996) but also as a competitive imperative (Porter 2001). The technologies that enable networks of firms to collaborate operationally have also been applied to develop electronically coordinated market institutions such as e-procurement.

Supply chain management started to develop as an area of significant academic enquiry in the early 1990s. The domain of enquiry and subject matter in this field is extremely diverse and continues to broaden. Topics of primary enquiry in the field, such as ISCM, relationship management, organisational behaviour and social, ethical and environmental supply issues, have developed their own agendas and sub-disciplinary debates (Chicksand et al. 2012, p. 455). Lamming (1996) argued that ISCM is an important theory within the field of PSCM. In their extensive analysis of the literature in the field, Richey et al. (2010) and Defee et al. (2010) both identify ISCM as the prevalent theory in supply chain management research.

The importance of integration to supply chain management has been widely recognised and is explicitly indicated by supply chain management definitions. For example, Cooper et al. (1997, p. 13) define supply chain management as:

> the integration of key business processes from end-users through original suppliers that provides products, services and information that add value for customers and other stakeholders.

Lambert (2004) defines supply chain management as:

> the cross-functional integration within the firm and across the network of firms that comprise the supply chain.

The Council of Supply Chain Management Professionals (CSCMP) also has the same emphasis in their definition of supply chain management:

> In essence, supply chain management integrates supply and demand management within and across companies.

ISCM continues to be a key theme among those seeking to understand how to harness the potential of the supply chain to create sustainable value. The notion of leveraging linkage and partnership within the supply chain is not new and can be traced to Heskett (1977) and identifies and operationalises the contribution of linking operational and cross-functional logistics activities as a way to improve corporate performance. Porter's (1985) value chain model also emphasises the importance of exploiting both intra- and inter-firm cooperation and linkage. In recent years, several important studies have contributed to better understanding of the key mechanisms for implementing ISCM (Lee and Whang 2000; Mentzer 2001; Lambert 2004; Stonebraker and Liao 2004; Lee et al. 2007; Chen et al. 2009; Childerhouse and Towill 2011). According to the synthesis of existing literature, it is suggested that information and communication technologies (ICTs) are the driving force behind implementing ISCM.

1.2 ICTs for Managing Supply Chains

In recent years, both manufacturing and service organisations have developed business models where they rely on a network of suppliers for a larger portion of product/service value (Persona et al. 2007). The competitive landscape was shifted from competition between individual firms or activities to competition between supply chains as a collection of networks of firms by sharing information and integrating supply chain processes. Real competitive advantage, therefore, comes from being able to leverage collaborative relationships in the supply chain to drive optimal planning decisions across organisational boundaries. Christopher (2011) argues that the current trends towards much closer collaboration between supply chain partners, process synchronisation across multiple enterprises and flexible information sharing across the supply chain can be expected to continue for many years.

Numerous studies have specifically examined the influence of competitive pressure on the use of ICTs and Internet-based systems to share data for competitive advantage (Lee et al. 2000; Ranganathan et al. 2004; Derrouiche et al. 2008). ICTs and Internet-based information exchange systems are now one of the major tools available to business managers for achieving operational excellence, improving collaborative decision making and achieving competitive advantage (Laudon and Laudon 2011). A continuing stream of ICTs innovation is transforming the traditional business operations. The growth of enterprise-wide information systems with rich and quality data sharing means that managers no longer operate in a fog of confusion, but instead have nearly instant access to the operations information they need for accurate and timely decisions.

On the demand side CRM applications provide the technological interface with customers that can “close the loop” in terms of enabling collaboration (Kwon et al. 2007). Applications of this type have the capability to create links between supply and demand by connecting to ERP applications using middleware or enterprise applications integration (EAI) technologies to enable the realisation of a “demand chain” (Jüttner et al. 2007). The potential for operational improvement through such integration of the front and back ends of the business is amplified when data being captured through a CRM system are shared and can be accessed by trading partners in the supply chain (Lee et al. 2000; Lin and Tseng 2006). Therefore, management of operations within the firm and the extended supply chain could be expected to benefit from greater data visibility and flexibility in information sharing between trading partners. Jonsson and Mattsson (2013) argue that in the contemporary global supply chain information sharing enabled by ICTs and Internet-based information exchange systems is crucial to achieve ISCM regardless of whether the focus is on transactional efficiency or strategic relationship management.

1.3 Information-Sharing Challenges

Information and communication technologies are the driving force behind successful supply chains nowadays. Automatic identification (auto-ID) technology as the integral part of supply chain ICTs can be seen as the current big wave in managing contemporary logistics activities and data exchange. Auto-ID technology includes linear barcode, two-dimensional barcode (2D barcode) and radio frequency identification (RFID) as the key tracking and tracing SC applications. Other auto-ID applications comprise optical character recognition (OCR), biometric recognition and smart cards. Advanced tracking and tracing technology is critical in the current business environment either in response to legal or compulsory requirements or as a voluntary initiative to improve internal and external business processes. Recently, different business sectors such as telecommunications, healthcare, retail, construction, food, pharmaceutical, automotive and aerospace have shown greater interest in improving their supply chain traceability and visibility of assets, driven by the advancement in auto-ID technology, specifically RFID. RFID technology is a prominent area of supply chain ICTs that has attracted a lot of attention in research and development. Its contactless nature and potential for data processing and storage gives it many advantages over existing machine-readable auto-ID technology (e.g. barcodes, optical recognition charters). Efficient RFID tracking and tracing practices are able to ensure important business aspects, including ethics, authenticity, quality, safety, security and sustainability. RFID requires collaboration between supply chain partners to realise the benefits of this technology. Although there are a large number of useful applications for this technology, at the same time there are emerging information security and privacy concerns relating to how governments and businesses implement the technology, which may breach the principles of the data protection policies (Kirk et al. 2007).

RFID technology has inherent vulnerabilities making it susceptible to a broad range of security risks. Karygiannis et al. (2006) proposed an RFID risk model focusing on network, business process and business intelligence risks. Mitrokotsa et al. (2009) identified RFID security threats in three main layers: hardware layer, the communication layer, and the back-end layer. Given the current big wave of RFID applications as the integral part of supply chain ICTs, there has to be a thorough understanding of emerging RFID security threats and effective self-protection mechanisms against system failures and attacks.

The telecommunications industry is widely regarded as critical infrastructure which reaches deep into the daily circumstances of individuals, businesses, and governments. Telecommunications along with the energy sector, in fact, forms a foundation upon which all other critical infrastructure operates (Kroger and Zio 2011). Information security is a major concern related to RFID application in the telecommunications sector. The RFID system is vulnerable to several attacks, including attacking and modifying tag threat, denial of service (DoS) attack, traffic analysis threat and spoofing attack (Khor et al. 2011). The privacy threat is another concern that combines location threat, constellation threat, transaction threat, preference threat, and breadcrumb threat. Besides, RFID tags might be infected with viruses that might corrupt the back-end databases and result in great disruption. The failure or damage to a telecommunications operator could disrupt services for thousands of phone customers, sever Internet connections for millions of consumers, cripple businesses, and shut down government operations. According to the Global State of Information Security Survey 2014, telecommunications operators are boosting information security and protection budgets significantly. The survey found that security budgets average US$5.4 million, a gain of 35 % on 2012. Overall IT spending climbed to an average of US$162 million for 2013, an increase of 17 % on the previous year. Secure control over RFID systems is still a challenge for telecommunications companies. Proposals have been introduced to overcome this concern.

2 Auto-ID Technology and SCM

This section discusses the main types of auto-ID tracking technologies. A comparison of these types of RFID tags is presented. Different auto-ID applications are highlighted with a special focus on supply chain management applications. This section ends with a discussion of the main challenges for auto-ID information security within a supply chain.

2.1 Auto-ID Systems

Automatic identification systems as part of ubiquitous wireless technologies can automate and streamline data entry, minimise human errors and labour costs, and provide accurate and up-to-date information fast (van Dorp 2002). The chief types of auto-ID technologies encompass linear barcodes, two dimensional (2D) barcodes, radio frequency identification (RFID) and other auto-ID technologies.

2.1.1 Linear Barcodes

One-dimensional barcode or linear barcode systems have been implemented in the retail sector since the 1950s (Bose and Pal 2005). Over the last 30 years, these systems have been used nearly everywhere in various types of businesses. The infrastructure for barcodes includes barcode tags, readers and a universal product code (UPC). Linear barcodes are seen as the simplest and lowest cost form of data capture technology implemented in tracking objects. The key advantages of linear barcode systems are that barcodes can be printed on durable substances and are not impacted by electromagnetic emissions or certain types of materials (White et al. 2007).

2.1.2 2D Barcodes

Two-dimensional barcodes, also called visual barcodes, have overcome the deficiency of one-dimensional barcodes that is mainly related to limited data storage. Two-dimensional barcodes are able to store, read, and process a big amount of information efficiently with no error in a small area (Gao et al. 2007). This type of barcode can support information detection, distribution and correction of errors with no need to access a database. The layout of linear barcodes differs from that of 2D barcodes (see Photo 1). Two-dimensional barcodes can be read in the most difficult environment and are more reliable due to their tolerance to damage, dirt and grease that facilitates its function to identify and correct errors (Swartz 2000). Two-dimensional barcodes facilitate identifying an object and allow interaction between the operator and the object. Therefore, 2D barcodes are used in transportation and warehousing to track shipping information that in most cases is separated from the products transported throughout the supply chain (Swartz 2000).

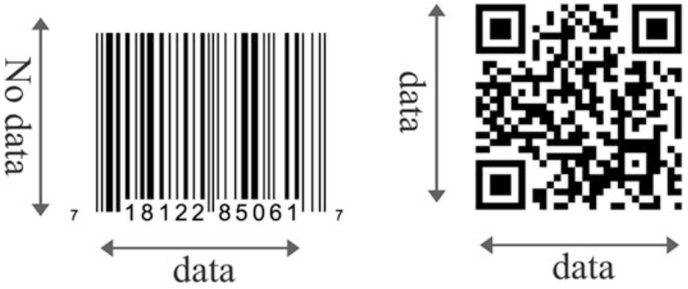


Photo 1 A 1D barcode stores up to 30 numbers, while a 2D barcode stores up to 7089 numbers (QRCode.jpg, tribalcafe.co.uk)

2.1.3 RFID

RFID is a term for any identification system wherein an electronic device which is attached to an object can communicate through radio frequency or magnetic field variations (Want 2006). RFID is seen as the next stage in barcode technology (Srivastava 2004). The RFID system consists of two key components: software and hardware. The hardware infrastructure includes tags or transponders, interrogators or readers and printers, and an antenna that is used in readers and tags (Glover and Bhatt 2006). The software infrastructure combines the tag's protocol, the reader's protocol, the RFID event manager or middleware to connect the RFID system to the

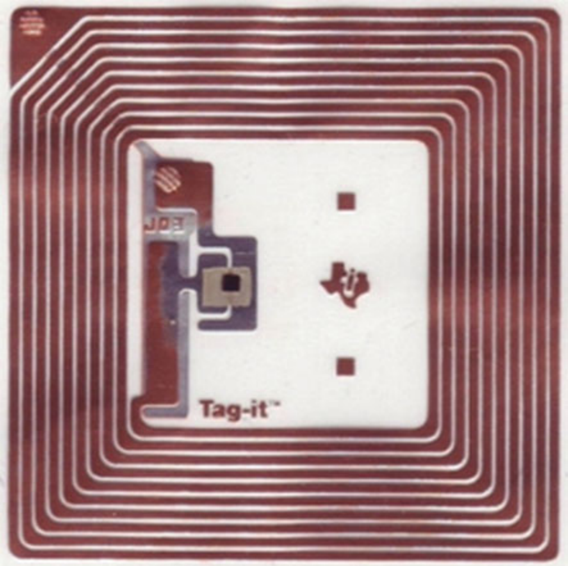


Photo 2 Smart label (www.100ups.com)

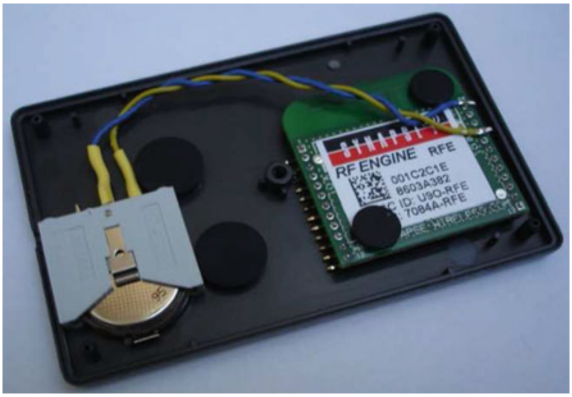


Photo 3 Active tag (www.truemeshnetworks.com)

Table 1 Specifications of passive and active tags

Criterion	Passive tag	Active tag
Power source	Operate without a battery	Powered by an internal battery
Power consumption	Lower power consumption	Higher power consumption
Read range	Smaller range	Greater range
Operating logic	Acquire power from the electromagnetic field generated by the reader	Internal power to transmit signal to the reader
Communication	Respond only	Respond and initiate
Reader	Require more powerful readers	Can be effective with less powerful readers
Noise	Subject to noise	Better noise immunity
Cost	Less expensive	More expensive
Sensitivity	Greater orientation sensitivity	Less orientation sensitivity
Design	Lower weight and smaller size	Greater weight and bigger size
Scope of reading	Fewer tags can be read simultaneously	More tags can be read simultaneously
Transmission rate	Lower data transmission rates	Higher data transmission rates
Longevity	Endless lifetime	Limited lifetime
Frequency rate	Lower frequency	Higher frequency
Memory	Less data storage	More data storage

Source Adapted from Glover and Bhatt (2006), Miles et al. (2010), Weis (2012)

bigger information system (Wyld 2006). An RFID tag is attached to an object as an identifier or identification device. The RFID reader is able to read the stored information on the tag. This information can be communicated between the RFID reader and another system that runs middleware located between RFID readers and applications (Glover and Bhatt 2006; Whitaker et al. 2007). There are three types of RFID tags according to the power source, including active, passive, and semi-passive (see Photos 2 and 3).

RFID technology represents a revolution in information and data exchange systems that enable the automated identification, tracking and tracing of every object from a source and factory to a customer through the use of a single tag on individual objects (Sellitto et al. 2007). RFID as a powerful trace technology is able to reduce uncertainty in managing supply chain and logistics activities compared to traditional barcode systems (Cannon et al. 2008). Table 1 contains a comparison between the specifications of passive and active tags. The downside of RFID technology is associated with setup and implementation costs, privacy and security concerns, reading issues and lack of universal standards (Michael and McCathie 2005).

2.1.4 Other Auto-ID Tracking Technology

- **Optical character recognition (OCR)**
  OCR is "the identification of printed characters using photoelectric devices and computer software" (Oxford dictionary 2012a). OCR is implemented as an easy and a quick means to transform hard copies, e.g. printed documents and books, into soft copies, i.e. electronic and editable files, for dissemination and processing. This allows printed texts to be published on a website or a computerised version of a manual/printed record-keeping system to be created. OCR as identification technology can also be used in identifying containers used in air and sea shipping (Bollen et al. 2004). An innovative application of OCR is the use of special scanners that are able to scan pages and convert them to spoken words. OCR is used in production, service and administrative fields.
- **Biometric technology**
  Biometric tracking technologies measure an individual's unique behavioural or physiological traits to determine his/her identity.
  Biometric tracking technology has many applications in almost every area. The most popular applications of biometric tracking technology include biometric devices for airport security, identification of DNA patterns for security, and other verification purposes, e.g. identifying criminals, biometric time and attendance systems to control timekeeping of employees, floor biometric security system for computer access and wireless biometrics for securer and safer transactions through wireless devices, and biometric locks and biometric safes such as smart floor systems (Anonymous 2005).
- **Smart/microprocessor cards**
  A smart card or a microprocessor card is "*a plastic card with a built-in microprocessor, used typically to perform financial transactions*" (Oxford dictionary 2012b). Smart cards are able to track and trace the information stored on the cards that vary from one application to another on the basis of the different arithmetic processing capacity and memory capacity. Smart cards are able to ensure a number of security aspects of stored and transmitted information related to integrity, privacy, authentication and confidentiality (Rankl and Effing 2010).

2.2 Auto-ID Applications

This section draws on a wide range of auto-ID applications with a special focus on RFID applications. RFID has been grouped as one of the ten most influential technologies in the 21st century (Chao et al. 2007). Auto ID technology covers extremely broad applications, including military logistics, transportation, healthcare, agriculture, games and sports, clothing, education, manufacturing, etc. (Li et al. 2006; Zhu et al. 2012). Many of these application areas span a number of firms

Table 2 Examples of auto-ID applications

Auto-ID application	Example
Identification and tracking	Livestock using rugged tags, pets with implanted tags, athletes in sports and games, children in theme parks, patients, passengers' luggage, medical equipment (e.g. in surgical medical products to ensure no items are left inside the patient during the operation), waste disposal, recycling, etc.
Access control for security and safety	Concert tickets, building access using RFID proximity cards, ski-lift passes, ignition keys of cars
Anti-counterfeiting	High-value currency notes, prescription drugs, luxury products
E-payment and stored-value systems	Automated toll-payment systems, contactless credit cards, stored-value cards, subway and bus passes, payment tokens (e.g. the Speedpass token for payments in petrol stations)

Source Adapted from Ilie-Zudor et al. (2011), Juels (2005), Li et al. (2006), Zhu et al. (2012)

in a logistical value chain. To enable the identification process, auto-ID systems offer unique identifiers or tags that are attached to objects. Technical feasibility and economy determine the choice of tag life cycle, including rewritability of tags, price, the details needed from the unique code, or the anticipated period of keeping unique identification information of an object (Ilie-Zudor et al. 2011).

Table 2 summarises the main dimensions of the general applications of auto-ID tracking technology.

2.3 Auto-ID Applications in Supply Chains

Advanced auto-ID technology, specifically RFID, is expected to cause the next revolution in supply chain management (Srivastava 2004). The capability of this technology is driven by data capture features such as reading speed, the need for line of sight, durability, quantity of data storage, human interaction and reusability of the data storage device (Asif and Mandviwalla 2005). RFID is able to improve efficiency in a supply chain in terms of cost and lead time reduction that in turn enhances a competitive position among its rivals (RFID Journal 2015).

Literature has indicated that among the core supply chain processes, advanced auto-ID applications, specifically RFID, have proved their concept in four key processes including demand management, order fulfilment management, manufacturing flow management and return management (Sabbaghi and Vaidyanathan 2008). It is argued that these four areas of supply chain management are able to add value throughout the entire supply chain by facilitating the mobility of critical items that encompass people, business activities, documents, information and communications (Keen and Mackintosh 2001). This highlights the influential role of RFID within supply chain processes.

2.3.1 RFID in Logistics, Warehousing and Transportation

The key benefits of using RFID in logistics are related to enhanced asset visibility and in turn more efficient operational practices. Auto-ID is an integral part for managing warehousing activities including receiving and check in, putting away and replenishment, order picking and shipment that result in more efficient activities (Angeles 2005; Michael and McCathie 2005).

RFID can also be used to support distribution and transportation processes with the support of other location-tracking applications such as GPS. These applications include logistics tracking, delivery security, automatic vehicle location, truck monitoring, courier parcel tracking, reusable asset tracking, tracking equipment data (e.g. forklifts and their batteries), air transportation and luggage handling and parcel delivery (Ilie-Zudor et al. 2011).

2.3.2 RFID in Retail

An important RFID application in the retail sector is the implementation of smart shelves at item level to avoid running out of stock of shelf items (Gaukler et al. 2007). These shelves have an RFID reader built in that can communicate with the inventory management system or ERP through middleware, hence shelf items' withdrawal and replenishment information is updated and in turn new orders are instigated at the right time. Therefore, RFID is a beneficial tool in improving operational efficiency through improved inventory management practices.

2.3.3 RFID in Manufacturing

As the core of supply chain activities, manufacturing and assembly have high potential for the implementation of RFID. The applications in manufacturing, assembly and configuration management aim to enhance the quality of products, especially those that are highly customised (Gaukler and Seifert 2007). Other industries that are concerned with pharmaceutical products, medical devices and electronics would gain the advantages of RFID technology for their manufacturing and assembly processes.

2.3.4 RFID for Security, Authentication and Counterfeit Protection

According to Gaukler and Seifert (2007), there are three mechanisms through which RFID can support counterfeiting protection and authentication of products, including the attendance of the RFID tag, the proprietary encoding on the chip of the RFID tag, and the establishment of a chain of custody that is also known as the e-pedigree of a product. RFID helps pharmaceutical companies to have a more secure supply chain against the risk of their products being counterfeited.

2.3.5 RFID Integrated with Environmental Sensors

RFID tags can be integrated with GPS sensors in major distribution hubs or in ports to enhance product security (Prasanna and Hemalatha 2012). Data of other environmental sensors (e.g. those related to temperature, humidity pressure, etc.) can be integrated and stored on RFID tags. Short shelf-life products such as perishable food, some pharmaceutical items and blood bags are sensitive to temperature and require cold conditions to be maintained. RFID systems can help to cut the spoilage cost through the ability to trace the history of the items, including the information about their physical status (Taylor 2014).

2.4 *Auto-ID Information Security Challenge*

This section demonstrates that successful implementation of innovative auto-ID technology requires trust in the technology in relation to the user community and that the technology is dependable and able to maintain this trust (Hutter and Ullmann 2005).

The EPC network as the most important industry standard for RFID sets how RFID data are transmitted from RFID readers to different applications as well as among applications in a supply chain. We identify the services that the EPC network offers to enhance routing and searching of EPC data, including the object name service (ONS), EPC information service, EPC discovery service (EPCglobal 2004).

Applying security controls to protect SCM applications is a complicated task due to the interorganisational nature of these applications using system-to-system networking. RFID-based EPC data are transmitted through RFID middleware and underlying servers located at various locations on the supply chain to EPC network services of supply chain partners (Stuart and John 2006).

In this section we discuss RFID information security threats that represent a major challenge for many businesses. Information security threats to RFID systems might be associated with the RFID reader, RFID tag, back-end system, link between RFID tag and RFID reader, link between back-end system and RFID reader (Huang 2009). These security threats are associated with integrity, authenticity, confidentiality and availability during the data exchange between the RFID tag and the RFID reader (Alfaro and Rabade 2009; Smart Border Alliance 2014).

2.4.1 Confidentiality Threats

The traffic between an RFID reader and a tag passes through an insecure wireless channel. Therefore, illegal collection of this traffic can theoretically occur through eavesdropping attacks. The motivation for confidentiality threats is rated as high because the dissemination of RFID information of an EPC network may be used by attackers to offer this information to thieves, competitors or any other party that has an interest in the tagged objects. The uniqueness of the data stored through an EPC results in unique tracking of objects/individuals carrying RFID tags.

2.4.2 Authenticity Threats

Attackers from outside who are able to use EPC Gen-2 can scan tagged objects that are in motion if they can manage to put a reader within the reading range of the tagged objects. The information stored on an EPC is the unique identification number of a certain object that travels across a supply chain. Any other information related to this unique number has to be retrieved by an EPC Information Service. If attackers can access the EPC data that use EPC codes, they can easily know the types and quantities of products in a supply chain. They can pass this information on to rivals or thieves. The attacker might get information such as product number and manufacturer from an EPC code that can be used by competitors for espionage purposes. In addition, attackers who can use the EPC codes scanned by an unauthorised RFID reader may clone or duplicate those tags by spoofing legal tags without accessing the organisation.

2.4.3 Integrity Threat

This threat is concerned with the possibility of attackers' adding, modifying, or deleting the information stored on the RFID tag. The aim of this attack is to disrupt business operations and to have a negative impact on revenue. Severe technical difficulties are expected from a proper integrity attack. The impact of this threat includes short-term disruption rather than major financial losses.

2.4.4 Availability Threats

Availability threats are associated with DoS attacks. The motivation for this attack is described as moderate in accordance with expected financial gains. Attackers might use two mechanisms to manage the target of a DoS attack. First, attackers might employ a compatible reader and work to kill a group of tags by sending kill commands. The technical difficulty of this attack is classified as strong because it is not easy to retrieve the destroyed information that was stored on the tag. Second, attackers may perform RFID jamming attacks to cause business disruption. Here, attackers from outside use powerful transmitters to jam the targeted readers' frequency. This attack is possible, yet solvable, because it is easy to find out the location of the transmitters.

Table 3 introduces an evaluation of RFID information security by considering different types of security threats.

Table 3 Evaluation of RFID information security

	Motivation	Difficulty	Likelihood	Impact	Risk
Confidentiality	High	Solvable	Possible	High	Critical
Authenticity	High	Solvable	Possible	High	Critical
Integrity	Moderate	Strong	Unlikely	Medium	Minor
Availability	Low	Strong	Unlikely	Medium	Minor

Source Alfaro and Rabade (2009)

3 Emerging RFID Security Challenges and Vulnerabilities

RFID technology is a prominent area of supply chain ICTs that has attracted a lot of attention in research and development for object identification as a ubiquitous infrastructure. Its contactless nature and potential for data processing and storage gives it many advantages over existing machine-readable auto-ID technology (e.g. barcodes, optical character recognition). Efficient RFID tracking and tracing practices are able to ensure important business aspects, including ethics, authenticity, quality, safety, security and sustainability. However, the working principles of RFID, such as contactlessness, lack of a clear line of sight, and the broadcast of signals, bring the security challenges and vulnerabilities, which disturb the reliability of RFID systems and block the deployment progress of RFID techniques. Although there are a large number of useful applications for this technology, at the same time there are emerging information security and privacy concerns relating to how governments and businesses implement the technology which may breach the principles of the data protection policies (Kirk et al. 2007). RFID technology has inherent vulnerabilities making it susceptible to a broad range of security risks. Karygiannis et al. (2006) proposed an RFID risk model focusing on network, business process and business intelligence risks. Mitrokotsa et al. (2009) identified RFID security threats in three main layers: hardware layer, communication layer, and back-end layer. Given the current big wave of RFID applications as an integral part of supply chain ICTs, there has to be a thorough understanding of emerging RFID security threats and effective self-protection mechanisms against system failures and attacks.

3.1 Technical Challenge

This section highlights the main technical challenges that hinder the deployment of RFID applications. These challenges include the lack of common standards and reading considerations. This section also explicates the factors that constrain RFID reading, including reading collision and signal interference concerns.

- ***Lack of common RFID standards***

To date, there are no general accepted standards for RFID. Common standards of RFID systems (i.e. tags, readers and frequencies) are required to gain maximum advantages across global supply chain trading partners (Li et al. 2006). The lack of common RFID standards is the key reason besides the high cost of technology for the elimination of its proliferation (Kay 2003). There are two international organisations that aim at developing global standards for RFID, including Electronic Product Code global (EPCglobal) and the International Standards Organisation (ISO) (Wu et al. 2006). For the UHF band, EPCglobal has developed the EPC class 1 G2 protocol, whilst ISO has released ISO-18000-6 standards. These two group of standards were under development and were not totally compatible with each other (Wu et al. 2006). RFID standards under both EPCglobal and ISO have now been standardised sufficiently, yet they are still not totally compatible (Ilie-Zudor et al. 2011).

Finally, certification procedures and power regulations are still incompatible among different nations (Wu et al. 2006).

- ***Reading considerations***

RFID reading is restricted by reading collision and signal interference problems. Reading collision is related to two key problems: RFID tag collision and RFID reader collision.

RFID tag collision occurs when a big number of tagged items are simultaneously interrogated by an RFID reader and send their signals back to the reader at the same time (Sellitto et al. 2007; Zhu et al. 2012). This causes confusion for the reader in a way that prevents it from scanning the tags and identifying items.

RFID reader collision is caused by simultaneous radio transmission causing overlapping among signals from various readers. When a large number of tags needs to be identified simultaneously, it is a serious concern if an RFID system cannot be completely accurate, because it is difficult to identify the tags that have failed to be read.

Other reading considerations are concerned with *material effects*. The ability of RFID readers to read through liquids and metals is poor, which leads to distortion of RFID signals (McGinity 2008). Finally, RFID readers can only read passive tags that are facing a particular direction, so objects should be packed accordingly.

3.2 Security Challenge

Information security is a major component of dependability of technology that represents a great challenge in such a pervasive complex computing environment (Hutter and Ullmann 2005). The core of the information security concept is authentication that indicates that a user is authorised to access a resource. If authentication is not established, information security cannot be maintained. From a

Table 4 RFID data security threats within a supply chain

	Inside the supply chain			Transition zone			Outside the supply chain	
Corporate data security threats	Manufacturing	Transportation	Distribution	Retail store	Store shelf	Checkout	World	Customer's home
	Corporate espionage threat							
	Infrastructure threat							
				Competitive marketing threat				
	Trust perimeter threat							
	Action threat							
Personal privacy threats							Association threat	
							Location threat	
							Preference threat	
							Constellation threat	
							Transaction threat	
							Breadcrumb threat	

Source Garfinkel et al. (2005)

supply chain perspective, RFID security threats can be classified in terms of corporate data security threats and personal privacy threats (Garfinkel et al. 2005) (see Table 4). Privacy threats are discussed in more detail in Sect. 3.4. This section adopts a system perspective to demonstrate different features of RFID security challenges.

RFID security threats are introduced based on a taxonomy model that considers the components of an RFID system.

The taxonomy model of RFID security threats consists of two levels (see Fig. 1). In the first level, the classification of the threat is based on the security property that the threat violates (Avoine and Oechslin 2005). These security properties are related to the three layers of the RFID communication model. The second level is concerned with the threats that are classified according to the system-specific attack types.

3.2.1 Application Layer Threats

A number of threats violate the properties of applications, including tag identification, personal privacy and back-end database operations (Rhee et al. 2005). These threats associated with the application layer include spoofing, replay, tracking, desynchronisation, and virus.

- **Spoofing attack**

A spoofing attack happens when a fake tag acts as a valid tag in a way that allows it to acquire services or products with someone else's identification (Peris-Lopez et al. 2006). When this identification is read, it is seen as a valid tag. This threat may affect digital passport systems, building access control systems and contactless payment systems (Zhen-hua et al. 2008).

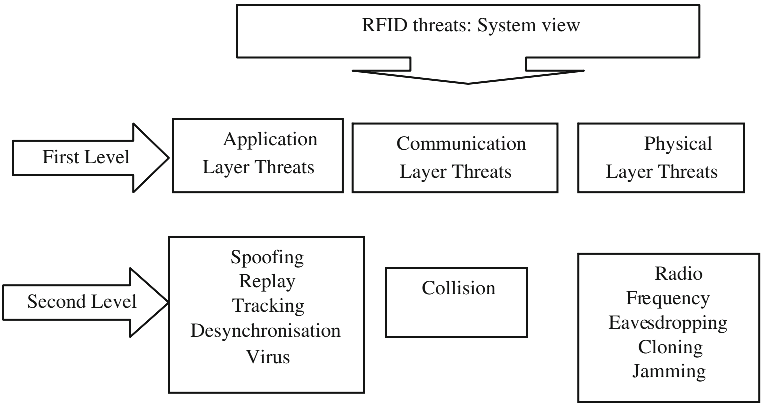


Fig. 1 RFID threats: system view

- **Replay attack**

Replay attacks harm the whole RFID system by consuming the computing resources of the reader, the tag and the back-end database system (Rieback et al. 2006). This attack causes misreading of some tags in the electromagnetic field of the RFID reader.

- **Tracking attack**

A tracking attack is a threat that targets personal privacy. RFID readers read and record unique tag identifiers that are associated with personal identities. This threat occurs when individuals are purposely tracked. The RFID privacy concern is explained in detail in the following sections.

- **Desynchronisation threat**

Desynchronisation is the threat of desynchronising the identification between an RFID tag and a back-end database server that can disable the tag (Lee 2005). Desynchronisation attacks damage the process of writing the ID of the tag. Besides, the writing process may fail if the connection between the reader and the back-end server is broken.

- **Virus**

In a case where the RFID tag gets infected with a virus, this RFID virus may use the injection of SQL to attack the back-end servers, which in turn results in failure in the entire RFID system. To prevent an RFID virus, the filter function in the RFID reader or middleware is used.

3.2.2 Communication Layer Threats

A collision attack is the chief threat of the communication layer that violates or interferes with the communication mechanism through which the RFID reader singles out a specific tag (EPCglobal Inc. 2005). The collision happens if more than one tag responds simultaneously to the interrogation of the reader. The attacker acts as one or as a number of tags respond at the same time to the interrogation of the reader (Feng et al. 2006).

3.2.3 Physical Layer Threats

The physical layer threats encompass radio frequency eavesdropping, cloning and jamming. These threats violate the electromagnetic properties of the RF signal in the physical layer (e.g. the carrier and the frequency clock cycle).

- ***Radio frequency eavesdropping***
  RFID is a wireless technology that is vulnerable to the risk of radio frequency eavesdropping between tags and readers. In this type of attack, the attacker

employs an antenna to record the signal between a reader and a legitimate tag in the same frequency, the antenna was already connected to a digital oscilloscope to capture the radio frequency signals collected by the antenna. Passive RFID systems are more vulnerable to this type of risk because they depend on the use of narrowband radio frequencies (Yu et al. 2006). If the encoding specification is known to the attacker, the signal picked up may have crucial implications due to the possibility of other attacks.

- ***Cloning***
  Low-cost, simple RFID tags are vulnerable to the risk of reverse engineering of a tag captured physically (Zhen-hua et al. 2008). In the cloning process, the attackers may analyse the carrier clock cycle, the signal's autocorrelation, and the encoding method, etc. Basic cloning does not need a deep view into the tag's ID structure. In the case of basic cloning, looking deliberately into the tag's ID structure is not required. Tag cloning is about determining the signal transmitted by the RFID tag and copying that signal. A spoofing attack is an RFID threat caused by cloning.
- ***Jamming/interruption***
  Noise signals cause jamming or interruption. The attack device is able to actively broadcast radio frequency signals in a way that can disrupt and block the operations of any close RFID readers (Xiao et al. 2007). Effective disruption might happen when using other patterns of modulation that are commonly used with jamming. The impact of jamming might be fatal in some instances, such as a disruption during the reading of medical data stored on an RFID tag. The threat that is associated with jamming is called desynchronisation.

3.3 Privacy and Regulatory Challenge

Privacy has been a major challenge for RFID applications that are associated with individuals who purchase products containing RFID tags. This section discusses different forms of personal privacy threats. This section also highlights the key challenges for developing RFID regulations to ensure RFID security and privacy.

3.3.1 Privacy Challenge

Privacy threats are associated with tracking attacks that were previously discussed in Sect. 3.3. The association between the RFID tags that have unique identifications and a person's identity enhances the risk of violating personal privacy (Garfinkel et al. 2005). Privacy objectives are concerned with protecting the data privacy and the location privacy of individuals (Smart Border Alliance 2014). Privacy threats comprise action, association, location, preference, constellation and transaction and breadcrumbs.

- **Action threat**
  This threat occurs when individual's behaviour is inferred by monitoring a group of tag actions. For example, the sudden disappearance of high-value items on smart shelves might indicate the possibility of shoplifting and results in the taking of a person's photograph.
- **Association threat**
  The association between an EPC-tagged product that the consumer purchased and the electronic serial number of the item causes this threat. The EPC links the consumer with a specific item rather than with a group of items. This kind of association can be involuntary and covert.
- **Location threat**
  Placing hidden readers at certain locations causes two types of privacy threats. First, a person carrying unique RFID tags can be tracked and his/her location can be revealed if a monitoring agency can associate tags with individuals. Second, the location of tagged items is susceptible to unauthorised disclosure.
- **Preference threat**
  According to the EPC network, the RFID tag attached to an item uniquely identifies the product type, the manufacturer and the item's unique identity. This is also associated with a value threat if the monetary value can be determined by the attacker.
- **Constellation threat**
  RFID tags form a constellation or a unique RFID shadow around the person. Without knowing their identities, attackers may use this RFID shadow or constellation to track people.
- **Transaction threat**
  During the movement of tagged items from one constellation to another, a transaction can be inferred between the persons associated with those constellations.
- **Breadcrumb threat**
  This threat is a result of the association between RFID tagged items and individuals' identities. When individuals collect tagged items, an item database that includes their identity in the firm's information system is built. This database is called an electronic breadcrumb. Removing the electronic breadcrumbs cannot break the association between the individuals and the items. This threat occurs when removed breadcrumbs are used.

3.3.2 Regulatory Challenge

This section explains the key challenges for developing RFID regulations to ensure RFID security and privacy. These regulations should be able to ensure that attacks must be intercepted, access controlled, data authenticated and the privacy of individuals guaranteed (Weber 2010). The nature of RFID systems requires a differentiated and heterogeneous legal framework that takes into consideration the verticality, globality, ubiquity and technicity aspects. It is stated that academic and regulatory proposals that deal with discrimination, security, privacy and consent have been ignored over last decade (Peppet 2014).

Regulation and legal aspects should be considered as a protection mechanism against RFID privacy concerns. Although privacy laws, acts and regulations are a powerful legislative mean, they have a number of challenges:

1. Detection of attacker: Legislative and regulatory restrictions are valuable when an attacker can be detected and brought to justice as a result. In ubiquitous systems, it is often very difficult to detect a violator of privacy regulations. The situation is much more difficult in RFID systems because of the wide distribution and the number of end devices that create a great challenge for the enforcement of privacy laws and regulations.
2. Globality: National legislation as well as self-regulation may not be sufficient or appropriate to ensure effective security and privacy (Weber 2010). There can be significant differences in privacy regulations and laws across countries. For instance, the legislation on privacy in US follows a sectoral path where there are separate regulations for each sector such as healthcare, industry, finance, etc. (Mark 2005). In contrast, the legal frameworks of the European Union, Canada and Australia have a cross-sector perspective to privacy legislation (European Parliament and Council Directive 1995; Paul et al. 2002). Furthermore, privacy legislations in the Third World countries vary widely and are not clearly identified. The globality challenge raises a concern of international interoperability related to legal privacy laws and regulations across countries. International legislations integrated with the detailed regulations of the private sector might be the best solution.
3. The outsourcing problem: This problem is related to the globality challenge of privacy legislation that creates more cases of law bypassing (Gudymenko 2011). For example, the lack of privacy regulations in some countries results in outsourcing problems.
4. Inherent inflexibility: Privacy regulations and laws are quite inflexible in certain situations. First, it is extremely complicated to have a legal framework that would be generic as well as detailed enough to cover the specialities of some use cases. Thus, most privacy regulations and laws are inflexible. Besides, to develop a new law or to introduce new amendments that provide new privacy regulations or acts, it takes time. That constrains the rapid response of legal enforcement to technological changes.
5. Ambiguous definitions: The number of definitions that are used in legal frameworks of privacy are vague. In some situations, it is not easy to link these definitions to technology aspects to get a clear interpretation.

4 RFID Applications in Telecommunications

This section discusses RFID applications in the telecommunication industry. In this section, the changes and transformations in the telecommunication industry that supported the deployment of RFID technology is discussed. Besides, this section identifies the benefits telecommunication companies can gain from implementing RFID technology in their supply chain.

Telecommunication companies are seen as customers of RFID services as well as RFID solutions providers (Wasserman 2007). RFID has a wide range of applications that can be implemented in different industries to enhance corporate performance and supply chain and logistics activities. However, some of these applications are not applicable in the telecommunications sector that represents a service-oriented business model.

RFID has several useful applications that help telecommunications companies to manage their assets throughout their life cycles. These applications can be categorised into three identification and tracking groups, including product, package and shipment (Fox 2005).

4.1 Product Identification and Tracking

Table 5 introduces different RFID applications in telecommunications in relation to product identification and tracking.

4.1.1 Telecommunications Product Package Tracking

RFID can be used to track reusable packages. RFID tags are embedded in the printed product package labels, ensuring that the information on the embedded RFID tag and that on the printed product label matches the product that is included in the package. If the RFID tag cannot be attached to the product, it might be applied to the product's package. The information stored on package RFID tags includes item identification, unique serial identification, quantity, CLEI code, country of origin, condition (i.e. defective/working) and net weight.

4.1.2 Shipping Data and RFID Tracking

As in packaging systems, RFID tags can be used in combination with barcodes to track pallets and containers that are shipped throughout a telecommunications supply chain. This requires the use of thermal transfer printers that allow writing to RFID tags that will be attached to the back of the label. Here the design of the antenna is critical and depends on the characteristics of the product that could affect the readability of an RFID tag that is attached to it.

Table 5 Product identification and tracking RFID applications in telecommunications

RFID application	Details
Labour-free inventory	Storing all plug-in cards that are not currently in use and are stored in a warehouse or a distribution centre by sending a request to the RFID system to give this information
Tracking defective plug-ins	When removing a defective plug from service, an update to the RFID system occurs to know that the plug is not usable
Automated database update without manual scanning	An automatic update occurs to the database when a plug-in card is removed from service and placed in a storage location
Tracking service trucks	RFID read/write tags can be used to track service trucks. The inventory of trucks can be read passively and related data can be transmitted to a central database through satellite link or mobile phone
Eliminating or minimising false dispatches	Accurate tracking of service trucks results in substantial savings on wrong dispatches. The RFID system allows automated checking to ensure that the right plug-ins are loaded prior to dispatch
Minimising network outages	The RFID tracking system helps maintenance staff to locate a required plug-in card across the network, find and install the card in an efficient and timely manner that minimises outages
Diminishing warranty and repair costs	The availability of the warranty information recorded in the plug-in cards helps to decrease repair costs and time
Tracking life-cycle information	RFID tracking information helps telecommunications companies to comply with compulsory product recovery rules in Jaban and Europe related to gathering end of life information that facilitates the recovery of disassembly and internal and external design information

Source ETSI (2006), Fox (2005)

4.2 *Implementation Challenge*

This section deals with RFID implementation challenges in the telecommunications industry. This section focuses on financial, technical, security and regulation challenges from a system point of view.

4.2.1 Financial Challenge

- The cost of RFID tags is still high compared to other tracking applications;
- Set up and migration costs of RFID system are relatively high.

4.2.2 Technical Challenge

- Telecommunications cards are quite small, leaving a tiny space for RFID tags. The RFID tag might be 25 mm^2. A tag circuitry might be installed on the cards themselves. In this case, testing is required to be done to avoid any negative effects on the equipment (ETSI 2006);
- Tests are required to check the distance at which RFID tags are readable. The effectiveness of RFID tags is negatively affected by the small size of the antenna and the use of metal materials;
- Due to the presence of RFID tags on telecommunications equipment, items in locations where various identification tools are implemented (such as barcode/2D labels or human readable labels) require process improvement analysis to ensure the suitability of RFID tags for current equipment;
- Interference with different requirements or equipment. For example, some transmitting devices such as wireless phones may adversely affect the operational performance of telecommunications equipment;
- Telecommunication companies face a technical challenge related to power limitations and the discrepancies in the allocation of regional frequency;
- Reading reliability is an important technical concern that is associated with the accuracy of reading all tags simultaneously;
- Testing is needed to check the impact of RFID signals within an exchange/central office location;
- Decentralisation of the telecommunications industry and the lack of one point of control constitute a security challenge in relation to encryption, information privacy and network security (Steinauer et al. 1997). This requires a high level of cooperation between industry and a government to develop new policies and practices to overcome security challenge.

4.2.3 Regulatory and Environmental Challenge

- The global nature of the telecom sector, different laws and regulations in each country that industry members should follow while incorporating the rules of a voluntary domestic framework. In general, the legal aspects of telecommunication interception is controlled by the law of the country where the interception happens (Campbell 2009);
- Other RFID implementation challenges include the diversity of the communication industry, the unprecedented changing rate of technology adopted by the sector's employees, customers and the IT and network facilities providers and the vulnerabilities associated with adopting new technologies (US Telecom Association US Telecom Association 2014);

- From an environmental and health perspective, there is a debate related to the environmental and health impacts of radiofrequency radiation from the telecommunications industry (Campbell 2009). The worry is that radiofrequency radiation may cause human cancer. Scientific health risk analysis is needed to provide a certain answer to this debate.

4.3 RFID: Availability Versus Confidentiality

This section illustrates the security objectives that telecommunication companies endeavour to achieve to overcome RFID security threats. This section also explains the impacts of RFID threats on attaining these objectives that help a firm to decide which security threat needs to be dealt with.

The security objectives that telecommunication companies endeavour to achieve to overcome RFID security threats include confidentiality, availability, integrity and authenticity (Smart Border Alliance 2014).

4.3.1 Confidentiality

The confidentiality objectives of the RFID system encompass the following elements:

- Unauthorised access should be prevented to ensure the protection of all data within the system;
- Unauthorised access should be prevented to ensure the protection of communications channels within the system;
- Unauthorised RFID reader access should be prevented to ensure the protection of the data on the RFID tags;
- The algorithm for developing unique identifiers should not be reverse engineered from known identifiers.

4.3.2 Integrity

The integrity objective of the RFID system entails a number of mechanisms, including:

- The protection of RFID tag data from unauthorised modification;
- The protection of data within the system from unauthorised modification;
- Preventing the duplication of RFID tags.

4.3.3 Availability

The requirements of availability that are related to the RFID system include:

- The existence of numerous tags should not result in system outage;
- The existence of many readers should not result in system outage;
- All components of the system are operational all the time;
- Multiple authorised individuals can access data from the back-end enterprise system that is available at any time.

4.3.4 Authenticity

This objective is associated with the assurance that a recipient or a sender cannot refute data transmissions and data modifications (van Deursen and Radomirovic 2009). The requirements for non-repudiation include:

- Mutual authentication should occur between the RFID reader and the RFID tag;
- Mutual authentication should occur between the middleware and the RFID reader.

This section also explains the impacts of RFID threats on attaining these objectives that help a firm to decide which security threat needs to be dealt with. This in turn depends on a firm's decision on the priority of achieving these objectives in relation to the implemented RFID system (Spruit and Wester 2013).

In considering the effects of RFID threats to the security objectives of information within a RFID system, Table 6 shows the negative effect of each RFID threat on information security objectives.

A threat to confidentiality negatively affects sensitive information through eavesdropping, a threat to availability will make important information, control and performance resources unavailable, and a threat to integrity will endeavour to control critical information, software or hardware resources (Alcaraz and Zeadally 2015).

Table 6 Negative impacts of RFID threats on information security objectives

RFID threats	Information security objectives		
	Confidentiality	Availability	Integrity
Eavesdropping data	X		
Eavesdropping transmission	X		
Spoofing	X		X
Cloning	X		X
Denial of service		X	
Tracking	X		

Source Spruit and Wester (2013)

This overview helps telecommunication companies to quickly decide which threat needs to be countered. To this end, a telecommunication company first has to decide on the priorities of information security objectives for its RFID system that requires protection.

4.4 Security Control Proposals

The literature review has proposed a number of solutions and mechanisms that can be implemented in different industries including telecommunications to overcome the privacy and security concerns. This section provides an overview of these suggested mechanisms. These solutions are categorised into two groups: cryptographic and non-cryptographic (Spruit and Wester 2013). The former offers more flexibility for privacy and security while the RFID tag moves between various owners. The latter is more efficient in dealing with RFID threats, yet it has some limitations related to how it can be implemented. The cryptographic security control capabilities include anonymous-ID scheme, public key (re-)encryption, hash lock, randomised hash lock, hash chain scheme, pseudonym throttling and delegation tree authentication. On the other hand, non-cryptographic protection capabilities comprise tag killing, tag locking, faraday cage, blocker tag and RFID guardian (Table 7).

5 Conclusion

5.1 Auto-ID/RFID Application Protection Mechanisms: A Conceptual Framework

This section develops a conceptual framework of RFID application protection mechanisms as an example of advanced auto-ID technology. In addition, three aspects of risk mitigation of RFID security threats have been identified that include management, operations and technology. This section demonstrates in detail the mechanisms of RFID application protection that are categorised into three groups constituting the proposed conceptual framework, including policy and legal propositions, operational security controls and technical countermeasures.

The objective of enhancing the protection of RFID systems requires collaboration among different stakeholders including infrastructure owners, governments and regulatory organisations, research and development centres, manufacturers, operators and users (Alcaraz and Zeadally 2014). Protection of advanced auto-ID systems requires risk mitigation that considers the value of information that needs protection. The National Institute of Standards and Technology (NIST) has classified risk

Table 7 The RFID security proposal: RFID threats and their protection countermeasures

RFID threats	Countermeasures											
	Cryptographic							Non-cryptographic				
	Anonymous-ID scheme	Public Key (Re-) encryption	Hash lock	Randomised hash lock	Hash-chain scheme	Pseudonym throttling	Delegation tree authentication	Tag killing	Tag locking	Faraday cage	Blocker tag	RFID guardian
RFID threats	X	X	X	X	X	X	X	X	X	X	X	X
Eavesdropping data								X		X	X	X
Eavesdropping transmission	X	X	X	X	X	X	X	X	X	X	X	X
Spoofing	X	X			X	X	X	X	X	X	X	X
Cloning								X		X	X	X
Denial of service												
Tracking	X	X		X	X	X		X		X	X	X

Source Roman et al. (2013), Spruit and Wester (2013)

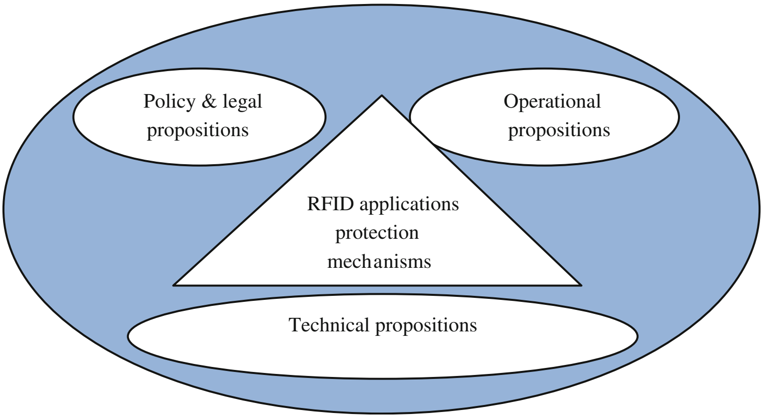

Policy & legal propositions
Operational propositions
RFID applications protection mechanisms
Technical propositions

Fig. 2 Auto-ID/RFID application protection mechanisms: a conceptual framework

mitigation measures into three aspects that include management security protection, technical and operational measures.

In this section we draw on these dimensions while developing a conceptual framework for RFID application protection (see Fig. 2).

5.1.1 Policy and Legal Propositions

Little work has been done in the area of developing policy propositions for the RFID system (Ayoade 2007). The literature has indicated a number of guiding rules for the implementation and deployment of RFID systems. Garfinkel et al. (2005) indicate that these guiding rules, "RFID Bill of Rights", will add to the tag's cost in the form of increased functionality or a battery. According to these rules, users and buyers of products with embedded RFID tags have the following rights:

1. The right to be informed if an RFID tag is embedded in a product;
2. The right to get RFID tags deactivated or removed when buying a product;
3. Consumers should not miss other rights if they decide to deactivate RFID tags or not to use RFID;
4. The right to be informed about the information stored inside their RFID tags. Erroneous information should be amended;
5. The right to know where, why, when an RFID tag is going to be read;
6. RFID tags should be embedded on product packaging and not on the product if possible;
7. RFID tags have to be visible and easily disposable.

It is claimed that compliance with RFID rules and regulations could be voluntarily adopted or legislated. If the former, conformance with rules could be attained through protocols, licensing logos, or intellectual property needed for appropriate RFID operations (Ayoade 2007).

5.1.2 Operational Propositions

This dimension of RFID application protection considers two points. First, information security measures in EPC network (see Table 8). Second, security controls for implementing RFID applications along with security metrics for measuring the performance of controls (Stuart and John 2006) (see Table 9).

5.1.3 Technical Propositions

The third pillar of RFID application protection mechanisms is associated with technical propositions that are introduced in Table 10.

Table 8 Proposed information security in EPC

Information security measures in EPC network	
Concern	Security considerations
RFID/EPC data	To maintain information confidentiality, authenticity, integrity and availability: All information related to EPC should be used by authorised persons behind firewalls; Sensitive information should be protected by a password; Confidential data should not be stored on RFID tags
EPC: information service (EPC-IS)	Security measures should be set up on the information system of a company that communicates with EPC-IS to manage and control the sharing and use of EPC data
EPC: discovery service (EPC-DS)	EPC-DS enables users to locate EPC data and to get access to these data through EPC-IS. Thus, security controls should be established for EPC-IS
Infrastructure hardware of EPC	RFID readers and tags constitute the EPC infrastructure hardware. The proposed security measures include: The data capturing process should not be designed to communicate completely meaningful information, i.e. only needed data are communicated, e.g. EPC ID, date, time and location of the read. This process should be implemented beyond the point of sales throughout supply chain checkpoints

Source Stuart and John (2006)

Table 9 Proposed security measures for RFID applications

Area of control	Mechanisms
Responsibility of information management	Individuals who have the right to manage information assets should have a clear definition of their roles and responsibilities
Categorisation of information	Personal and sensitive data should be categorised according to information security objectives including confidentiality, availability and integrity
Protection of process/information	Data protection requirements should vary according to the requirements of certain information security classifications. Data must be protected against unauthorised access from outside the business. Appropriate technical measures should be used to ensure that
Formal contracts for information distribution and transfer	A formal contract is required to allow a third party to access or transfer personal data
Virus control	Anti-virus control applications must be installed to protect all systems that are vulnerable to viruses
Password management	Password management is needed to control the use of: – Access/kill password of RFID tag; – Computing facilities password concerned with different EPC network services

Source Stuart and John (2006)

Table 10 RFID application protection mechanisms: technical propositions

Concern	Security propositions
Tag to reader authentication	Implementation of ID randomisation and hashing
	Implementation of mutual/bi-directional authentication
	Implementation of response/challenge protocol
Optimised radio frequency protocols	Allow very little information about RFID tag identity throughout operation
	Enhance the algorithms of collision-avoidance to eliminate data compromise
Data confidentiality	Development of efficient cryptographic techniques on tags
	Validate and store protected information on tags
High assurance readers	RFID readers should be designed with an efficient kill capability to enhance manageable passwords
	RFID readers should be designed to reliably and efficiently execute looking at read/write tags
	RFID readers should have the ability to execute evolving security and privacy policies
System security engineering	Implementation of highly developed identity and authentication management techniques
	Secure database architectures should be integrated with granular access control
	Highly reliable, secured and efficient computing systems should be designed
	Integration between existing privacy and security infrastructure and RFID systems should be established

Source Karygicmnis et al. (2006), Roman et al. (2013)

References

Alcaraz C, Zeadally S (2014) Critical infrastructure protection: requirements and challenges for the 21st century. Int J Crit Infrastruct Prot 8:53–66

Alcaraz C, Zeadally S (2015) Critical infrastructure protection: requirements and challenges for the 21st century. Int J Crit Infrastruct Prot 8:53–66

Alfaro J, Rabade L (2009) Traceability as a strategic tool to improve inventory management: a case study in the food industry. Int J Prod Econ 118(1):104–110

Angeles R (2005) RFID technologies: supply chain applications and implementation issues. Inf Syst Manage 22(1):51–65

Anonymous (2005) Applications of biometrics: area harnessing the technology. Available at http://www.questbiometrics.com/applications-of-biometrics.html. Last access 03 Feb 2012

Asif Z, Mandviwalla M (2005) Integrating the supply chain with RFID: a technical and business analysis. Commun Assoc Inf Syst 15(24):393–427

Avoine G, Oechslin P (2005) RFID traceability: a multilayer problem. In: Proceedings on financial cryptography, pp 125–140

Ayoade J (2007) Privacy and RFID systems: roadmap to solving security and privacy concerns in RFID systems. Comp Law Secur Rev Int J Technol Pract 23:555–561

Bollen F, Kissling C, Emond J-P, Brecht J, McAneney, Leake J, Compton R, Nunes C, Metz A, Duval K, Laniel M, Ye J (2004) Sea and air container track and trace technologies: analysis and case studies. Available at http://www.apec-tptwg.org.cn/new/Archives/tpt-wg23/Competitive/ITF/Draft-Final-Report2-Jun04.pdf. Last access 08 Jan 2012

Bose I, Pal R (2005) Auto-ID: managing anything, anywhere, anytime in the supply chain. Commun ACM 48(8):100–106

Campbell D (Ed) (2009) International telecommunication law. Yorkhill Law Publishing, Salzburg, p 2007

Cannon AR, Reyes PM, Frazier GV, Prater E (2008) RFID in the contemporary supply chain: multiple perspectives on its benefits and risks. Int J Oper Prod Manage 28(5):433–454

Chao CC, Yang JM, Jen WY (2007) Determining technology trends and forecasts of RFID by a historical review and bibliometric analysis from 1991 to 2005. Technovation 27(5):268–279

Chen H, Daugherty PJ, Landry TD (2009) Supply chain process integration: a theoretical framework. J Bus Logistics 30(2):27–46

Chicksand D, Waston G, Walker H, Radnor Z, Johnston R (2012) Theoretical perspectives in purchasing & supply chain management: an analysis of the literature. Supply Chain Manage Int J 17(4):454–472

Childerhouse P, Towill D (2011) Arcs of supply chain integration. Int J Prod Res 49(24):7441–7468

Christopher M (2011) Logistics and supply chain management: strategies for reducing cost and improving service, 4th edn. Pearson Education Limited/Financial Times Prentice Hall, Harlow

Cooper MC, Lambert DM, Pagh JD (1997) Supply chain management: more than a new name for logistics strategy. Int J Logistics Manage 4(2):13–24

Defee CC, Williams B, Randall WS, Thomas R (2010) An inventory of theory in logistics and supply chain management research. Int J Logistics Manage 21(3):404–489

Derrouiche R, Neubert G, Bourar A (2008) Supply chain management: a framework to characterize the collaborative strategies. Int J Comput Integr Manuf 21(4):426–439

EPCglobal Inc (2005) EPC™ radio-frequency identity protocols class-1. EPC Global Inc., New Jersey, USA

EPCglobal (2004) The EPCglobal network: overview of design, benefits and security. EPC Global Inc., New Jersey, USA

European Telecommunications Standards Institute (ETSI) (2006) Telecommunication and internet converged services and protocols for advanced networking (TISPAN). Overview of Radio Frequency Identification (RFID). Tags in the telecommunications industry. Technical Report: ETSI TR 102(449) V1.1.1, 2006–01

European Parliament and Council Directive (1995) Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281 (23/11):0031–0050

Feng B, Li JT, Guo JB, Ding ZH (2006) ID-binary tree stack anticollision algorithm for RFID. In: 11th IEEE Symposium on Computers and Communication. IEEE Press, pp. 207–212

Fox R (2005) Radio frequency identification (RFID) in the telecommunications industry: Telcordia. Available at http://www.commonlanguage.com/content/resources/commonlang/productshowroom/showroom/equip_id/carriers/eqpt_td_gen_wp_001.pdf. Last access 20 Apr 2015

Gao JZ., Prakash L, Jagatesan R (2007) Understanding 2D-barcode technology and applications in m-commerce-design and implementation of a 2D barcode processing solution. In: Proceedings of the 31st Anual international Computer Software and Applications Conference-COMPSAC, July 24–27, Washington, DC. IEEE Computer Society, Vol 2, pp 49–56

Garfinkel SL, Juels A, Pappu R (2005) RFID privacy: an overview of problems and proposed solutions. IEEE Comp Soc IEEE Secur Priv 3:34–43

Gaukler GM, Seifert RW, Hausman WH (2007) Item-level RFID in the retail supply chain. Prod Oper Manage 16(1):65–76

Gaukler G, Seifert R (2007) Applications of RFID in supply chains. In: Jung H, Chen F, Jeong B (eds) Trends in supply chain design and management: technologies and methodologies. Springer, London, pp 29–48

Glover B, Bhatt H (2006) RFID essentials, 1st edn. O'Reilly, Sebastopol

Gudymenko I (2011) Protection of the users' privacy in ubiquitous RFID systems. Master's dissertation, Technische Universität Dresden

Hammer M (2001) The superefficient company. Harvard Bus Rev 79(8):82–91

Helbing D (2013) Globally networked risks and how to respond. Nature 497:51–59

Heskett JL (1977) Logistics—essential to strategy. Harvard Bus Rev 55(6):85–96

Huang CH (2009) An overview of RFID technology, application, and security/privacy threats and solutions. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.175.9165&rep=rep1&type=pdf. Last access 19 Apr 2015

Hutter D, Ullmann M (2005) Security in pervasive computing. In: Second international conference, SPC 2005. Boppard, Germany, April 2005. Springer, Berlin

Ilie-Zudor E, Kemény Z, van Blommestein F, Monostori L, van der Meulen A (2011) A survey of applications and requirements of unique identification systems and RFID techniques. Comput Ind 62(3):227–252

Jonsson P, Mattsson S (2013) The value of sharing planning information in supply chains. Int J Phys Distrib Logistics Manage 43(4):282–299

Juels A (2005) RFID security and privacy: a research survey. Available at https://www.rsa.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf. Last access 21 Jan 2012

Jüttner U, Christopher M, Baker S (2007) Demand chain management—integrating marketing and supply chain management. Ind Mark Manage 36(3):377–392

Karygiannis T, Phillips T, Tsibertzopoulos A (2006) RFID security: a taxonomy of risk. In: Proceedings of the 1st international conference on communications and networking in China (China'Com 2006), October 2006. IEEE Press, pp 1–8

Karygicmnis A, Phillips T, Tsibertzopoulos A (2006) RFID security: a taxonomy of risk. Paper presented at the first international conference on communications and networking in China, 2006. ChinaCom'06

Kay E (2003) What's the next step for RFID. Frontline Solutions 4(3):21–25

Keen P, Mackintosh R (2001) The freedom economy: gaining the m-commerce edge in the era of wireless Internet. Osborne/McGraw-Hill, New York

Khor J, Ismail W, Younis M, Sulaiman M, Rahman M (2011) Security problems in an RFID system. Wireless Pers Commun 59(1):17–26

Kirk S, Fraser J, Vincenti J (2007) Is big business watching you? RFID tags, data protection, and the retail industry in the European Union. Comp Internet Lawyer 24(2):1–5

Kroger W, Zio E (2011) Vulnerable systems. Springer Publishing, Dordrecht

Kwon O, Im GP, Lee KC (2007) MACE-SCM: a multi-agent and case-based reasoning collaboration mechanism for supply chain management under supply and demand uncertainties. Expert Syst Appl 33(3):690–705

Lambert DM (2004) Supply chain management: process, partnership, performance. Supply Chain Management Institute, Sarasota

Lamming R (1996) Squaring lean supply with supply chain management. Int J Oper Prod Manage 16(2):183–196

Laudon K, Laudon J (2011) Management information systems: managing the digital firm, 13th edn. Pearson Education Limited/Financial Times Prentice Hall

Lee CW, Kwon IG, Severance D (2007) Relationship between supply chain performance and degree of linkage among supplier, internal integration, and customer. Supply Chain Manage Int J 12(6):444–452

Lee HL, Whang S (2000) Information sharing in a supply chain. Int J Technol Manage 20 (3/4):373–387

Lee S (2005) Mutual authentication of RFID system using synchronized secret information. Master's dissertation, School of Engineering, Information and Communications University

Li S, Visich JK, Khumawala BM, Zhang C (2006) Radio frequency identification technology: applications, technical challenges and strategies. Sens Rev 26(3):193–202

Lin CH, Tseng HJ (2006) Identifying the pivotal role of participation strategies and information technology application for supply chain excellence. Ind Manage Data Syst 106(5/6):739–756

Mark L (2005) Personal privacy in ubiquitous computing: tools and system support. PhD

McGinity M (2008) RFID not your father's Barcode, IEEE distributed systems online. Available at http://dsonline.computer.org/portal/site/dsonline/menuitem.9ed3d9924aeb0dcd82ccc6716bbe36ec/index.jsp?&pName=dso_level1&path=dsonline/2003_Archives/0308/f&file=newsp.xml&xsl=article.xsl&. Last access 13 Apr 2008

Mentzer JT (2001) Supply chain management. Sage Publications, London

Michael K, McCathie L (2005) The pros and cons of RFID in supply chain management (ICMB'05). In: Proceedings of the international conference on mobile business, IEEE

Miles SB, Sarma SE, Williams JR (2010) RFID: technology and applications. Cambridge University Press, Cambridge

Mitrokotsa A, Rieback MR, Tanenbaum AS (2009) Classifying RFID attacks and defenses. Special issue on advances in RFID technology, Information Systems Frontiers. Springer Science & Business Media, LLC 2009. doi:10.1007/s10796-009-9210-z

Oxford dictionary (2012a) Optical character recognition. Available at http://oxforddictionaries.com/definition/optical%2Bcharacter%2Brecognition?q=optical+character+recognition. Last access 23 Feb 2012

Oxford dictionary (2012b) Smart card. Available at http://oxforddictionaries.com/definition/smart+card. Last access 23 Feb 2012

Paul A, Calvin P, Matthias S (2002) From privacy promises to privacy management: a new approach for enforcing privacy throughout an enterprise. In: Proceedings of the 2002 workshop on new security paradigms, NSPW '02, New York, NY, USA, 2002. ACM, pp 43–50

Peppet SR (2014) Regulating the internet of things: first step toward managing discrimination, privacy, security, and consent. Texas Law Rev 93(85):85–178

Peris-Lopez P, Hernández-Castro JC, Estévez-Tapiador JM, Ribagorda A (2006) RFID systems: a survey on security threats and proposed solutions. PWC, pp 159–170

Persona A, Regattierri A, Pham H, Battini D (2007) Remote control and maintenance outsourcing networks and its applications in supply chain management. J Oper Manage 25(6):1275–1291

Porter ME (1985) Competitive strategy: creating and sustaining superior performance. The Free Press, New York

Porter ME (2001) Strategy and the internet. Harvard Bus Rev 79(3):62

Prasanna KR, Hemalatha M (2012) RFID GPS and GSM based logistics vehicle load balancing and tracking mechanism. In: International conference on communication technology and system design 2011, vol 30, pp 726–729

Ranganathan C, Dhaliwal JS, Teo TSH (2004) Assimilation and diffusion of wed technologies in supply chain management: an examination of key drivers and performance impacts. Int J Electr Commer 9(1):127–161

Rankl W, Effing W (2010) Smart card handbook, 4th edn. Wiley, West Sussex

RFID Journal (2015) RFID in consumer products. RFID J. Available at http://www.rfidjournal.com/faq/29/27. Last access 20 Apr 20 2015

Rhee K, Kwak J, Kim S, Won D (2005) Challenge-response based RFID authentication protocol for distributed database environment. In: International conference on Security in Pervasive Computing. SPC, Vol. 3450, pp 70–48

Richey RG, Roath AS, Whipple JM, Fawcett SE (2010) Exploring a governance theory of supply chain management: barriers and facilitators to integration. J Bus Logistics 31(1):237–256

Rieback MR, Crispo B, Tanenbaum AS (2006) Is your cat infected with a computer virus?. In: Proceedings of the 4th IEEE international conference on Pervasive Computing and Communications. IEEE Press, pp 169–179

Roman R, Zhou J, Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. Towards Sci Cyber Secur Identity Archit Future Internet 57 (10):2266–2279

Sabbaghi A, Vaidyanathan G (2008) Effectiveness and efficiency of RFID technology in supply chain management: strategic values and challenges. J Theor Appl Electr Commer Res 3(2):71–71

Sellitto C, Burgess S, Hawking P (2007) Information quality attributes associated with RFID-derived benefits in the retail supply chain. Int J Retail Distrib Manage 35(1):69–87

Smart Border Alliance (2014) RFID security and privacy. RFID feasibility study final report

Spruit M, Wester W (2013) RFID security and privacy: threats and countermeasures, technical report UU-CS- 2013-001. Utrecht, Netherlands: Department of Information and Computing Sciences, Utrecht University

Srivastava B (2004) Radio frequency ID technology: the next revolution in SCM. Bus Horiz 47 (6):60–68

Steinauer DD, Radack SM, Katzke SW (1997) U.S. government activities to protect the information infrastructure. Germany: Presented at the 5th Annual BSI IT Security Congress in Bonn, Germany (April 1997). Available at http://csrc.nist.gov/publications/secpubs/otherpubs/usgovII.pdf. Last access 21 Apr 2015

Stonebraker PW, Liao J (2004) Environmental turbulence, strategic orientation: modeling supply chain integration. Int J Oper Prod Manage 24(10):1037–1054

Stuart GK, John JL (2006) Security RFID applications: issues, methods and control. Inform Syst Secur 15(4):43–50

Swartz J (2000) Changing retail trends, new technologies, and the supply chain. Technol Soc 22 (1):123–132

Taylor JIM (2014) Enhance granularity of visibility in the food supply chain: use track and trace technologies. Food Logistics (Special report, 154), pp 30–32

US Telecom Association (2014) Experience with the framework for improving critical infrastructure cybersecurity: comments of the US Telecom association. Available at http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_ustelecom_scott.pdf. Last access 21 Apr 2015

van Deursen T, Radomirovic S (2009) Security of RFID protocols: a case study. Electr Notes Theor Comp Sci 244:41–52

van Dorp KJ (2002) Tracking and tracing: a structure for development and contemporary practices. Logistics Inf Manage 15(1):24–33

Want R (2006) An introduction to RFID technology. IEEE Pervasive Comput 5(1):25–33

Wasserman E (2007) Telcos' dual vision for RFID. RFID J, December 1st 2007, https://www.rfidjournal.com/purchaseaccess?type=Article&id=3806&r=%2Farticles%2Fview%3F3806. Accessed 20 Aug 2015

Weber RH (2010) Internet of things—new security and privacy challenges. Comp Law Secur Rev 26(1):23–30

Weis SA (2012) RFID (radio frequency identification): principles and applications. Available at http://www.eecs.harvard.edu/cs199r/readings/rfid-article.pdf. Last access 22 Jan 2012

Whitaker J, Mithas S, Krishnan MS (2007) A field Study of RFID deployment and return expectations. Prod Oper Manage 16(5):599–612

White GRT, Gardiner G, Prabhakar G, Abd Razak A (2007) A comparison of barcoding and RFID technologies in practice. J Inf Inf Technol Organ 2:119–131

Wu NC, Nystrom MA, Lin TR, Yu HC (2006) Challenges to global RFID adoption. Technovation 26(12):13–17

Wyld DC (2006) RFID 101: the next big thing for management. Manage Res News 29(4):154–173

Xiao Q, Boulet C, Gibbons T (2007) RFID security issues in military supply chains. In: Proceedings of the2nd international conference on Availability, Reliability and Security, pp 599–605

Yu P, Schaumont P, Ha D (2006) Securing RFID with ultra-wideband modulation. In: RFID Sec 2006, Graz, Austria

Zhen-hua D, Li JT, Feng B (2008) A taxonomy model of RFID security threats. ICCT, pp 765–776

Zhu X, Mukhopadhyay SK, Kurata H (2012) A review of RFID technology and its managerial applications in different industries. J Eng Tech Manage 29(1):152–167

Disrupting Terrorist and Criminal Networks: Crime Script Analysis Through DODAF Applications

Anthony J. Masys

Abstract The complexity of the current threat landscape associated with terrorism and criminal networks continues to be a top national and global security agenda item. With heightened awareness and concern regarding the proliferation and expansion of ISIL and connections to homegrown violent extremism, understanding the network structure and functional perspectives is a key enabler to supporting counter terrorism disruption strategies. Challenges associated with understanding these ‘dark networks’ stems both from contextualizing the information (plagued by uncertainty and ambiguity) and from the multiplex nature of the actors whereby they can share more than one type of relation. In this exploratory work, Counter-Terrorism Architectural Frameworks (CTAF) is introduced as an application of the Department of Defense Architectural Frameworks (DODAF) to support ‘opening the blackbox’ of terrorist activities to identify terrorist network vulnerabilities and to develop disruption strategies. The multiple views afforded by the application of DODAF provides a more comprehensive picture to support decision making and can highlight the complex organizational dynamics that are not readily observable through Social Network Analysis (SNA) alone. In this chapter the methodology is explained and applied to an analysis of the Lashkar-e-Taiba (LeT) terrorist network (Subrahmanian et al. in Computational analysis of terrorist groups: Lashkar-e-Taiba. Springer, Berlin, 2013) and the Noordin Top terrorist network (Roberts and Everton in J Soc Struct 12(2), 2011).

Keywords Social network analysis · Crime scripting · DODAF · Terrorism · ISIL

A.J. Masys (✉)
University of Leicester, Leicester, UK
e-mail: anthony.masys@gmail.com

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_11

1 Introduction

The current threat landscape associated with terrorism and criminal networks continues to be a top national and global security agenda item. As described in GTI (2014), '…in 2013 terrorist activity increased substantially with the total number of deaths rising from 11,133 in 2012 to 17,958 in 2013, a 61 % increase. Since 2000 there has been over a five-fold increase in the number of deaths from terrorism, rising from 3361 in 2000 to 17,958 in 2013'.

In particular the proliferation/expansion of ISIL and affiliates represents a national and global security issue. As described in The Economist (2015):

> When the jihadists of Islamic State (IS) seized Mosul and the Iraqi army fled last June, they became the world's most dangerous terrorist organisation. Sweeping out of Syria and north-western Iraq, they stormed southward, and came close to taking Baghdad. They murdered male prisoners in gory videos and enslaved female ones. Groups from Nigeria to Libya and Afghanistan pledged allegiance to them. Devotees attacked innocent civilians in Western cities; this week at least 19 people were killed in an assault on tourists in Tunisia (though the culprits are unknown).

Visual thinking and analytical approaches afforded by Social Network Analysis (SNA) is playing an increasingly prominent role in the intelligence community with a focus on terrorism, insurgency and organized crime groups. A terrorist network can be modeled as a generalized network (graph) consisting of nodes and links (Fig. 1). Nodes are actors with specific attributes. Links between actors represent a relation. These relations are more than connectivity but have a specific context and property. The relations that connect the actors of a network can represent communication, formal relations, material or work flow ties and proximity ties. To analyze the network, centrality measures and clustering algorithms reveal insights regarding the relative importance of different individuals or different parts of the network (Fig. 4). The complexity of such networks is not only associated with the static interdependencies but also in the dynamics, as terrorists establish new relations or break existing relations with others, their position roles, and power may change accordingly (Aghakhani et al. 2011: 192).

Understanding not only the network structure but also the functional 'activity networks' is required to strategically target and disrupt these dark networks. Functional mapping of terrorist networks and criminal organizations captures the activities, value chains and operating logic models to support a more comprehensive understanding of these networks. Understanding how these networks function

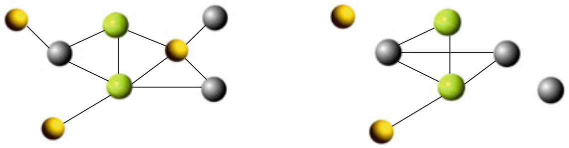


Fig. 1 Social network examples (nodes and links)

(crime scripting) provides context to the social network analysis and the underlying dynamics and transition points of the terrorist network from planning to operations.

As noted by Roberts and Everton (2011: 8): '…terrorist analysis requires an approach that recognizes and embraces the multi-relational, multi-layer, and multi-metric analysis of a terror network'. The purpose of this chapter is to present a crime scripting approach 'Counter Terrorism Architectural Frameworks (CTAF)' as a methodology to support network analysis for counter terrorism disruption strategies and to facilitate understanding regarding resiliency, stability and fragility of terrorist networks.

2 Network Analysis

Social network analysis is an approach to facilitate understanding of a group of 'actors' through a structured analysis that leverages the domains of mathematics, anthropology, psychology, and sociology. The methodology and visual thinking approach focuses on uncovering the patterning of people's interaction and interpreting the network attributes to facilitate better understanding regarding the behavior of the network. In light of this, Network analysis has been instrumental in analyzing terrorist and criminal networks (Masys 2014a). By connecting the dots, the methodology provides insights into the 'dark' network through:

- Centrality analysis: determining more important actors of a social network so as to understand their importance or influence in a network.
- Community detection: identify groups of actors that are more densely connected among each other than with the rest of the network.
- Information diffusion: studies the flow of information through networks.
- Link prediction: aims at predicting for a given social network how its structure evolves over time, that is, what new links will likely form.
- Generative models: probabilistic models which simulate the topology, temporal dynamics and patterns of large real world networks.

Social networks are normally represented as graphs (Fig. 1). A graph G (V, E) consists of a set of nodes V and a set of edges E (either directed or undirected).

SNA relies to a large extent on a mathematical model in the form of a graph and a set of algorithms that traverses the graph in various ways to analyse the network. This is described well in Carrington et al. (2005), Easley and Kleinberg (2010), Gunduz-Oguducu and Etaner-Uyar (2014), Wiil (2011) and Masys (2014a). Key analysis metrics described in the domain of SNA include:

- Size
- Density
- Cluster
- Average shortest path
- degree centrality

- closeness centrality
- betweenness centrality
- Eigenvector centrality

Such measures can be used to support terrorist targeting. However, new insights from social network analyses emphasize that the fluidity and flexibility of the social structure of criminal networks makes them highly resilient against traditional law enforcement strategies. For instance, 'it was found that even though a drug trafficking network was structurally targeted over a substantial period of time, the trafficking activities continued and its network structure adapted. Research concerning the resilience of criminal networks involved in the production of ecstasy in the Netherlands lead to the same conclusions' (Duijn et al. 2014: 1). Such network resilience leads to the requirement to better understand the relational and actor context 'crime scripts' associated with the network to facilitate strategies for disruption.

3 Crime Script Analysis

It is not enough to just understand the existence of connections between actors in a criminal or terrorist network. Context is a key attribute. Crime script analysis is a methodology that supports contextual understanding of criminal networks. According to Levi and Maguire (2004), crime scripts are an innovative way to gain a more detailed understanding of complex forms of crime and design prevention measures. Crime scripts map the sequence of actions used by offenders during crime commission. The potential for crime scripts to capture the sequential detail of crime-commission processes is important for understanding complex crimes, such as the operations involved in drug laboratories, human trafficking, financial and cyber crime. Crime scripts include the events that occur prior, during and after an event, or series of events.

This understanding is necessary for designing strategic prevention measures that have lasting reduction effects on crime. In capturing the sequence of actions and decisions before, during and after a crime, crime script analysis capture the full range of possible intervention points (Chiu et al. 2011: 356) as described with regards to clandestine drug laboratories (Chiu et al. 2011) and with regards to Italian mafia and scripts of human trafficking for sexual exploitation in Italy (Leclerc 2014).

Crime scripting shows value for counter-terrorism operations through its inherent ability to support the design of prevention strategies by revealing potential 'dark network vulnerabilities'. Such interventions can disrupt terrorist operations by reducing opportunities and resources and removing key actors from the network thereby increasing risks associated with the commission of a terrorist act (Chiu et al. 2011: 359).

4 DODAF

The **Department of Defense Architecture Framework** (**DODAF**) is an architecture framework utilized by the United States Department of Defense (DoD) that provides a multiple perspective (views) of an infrastructure. These views are artifacts for visualizing, understanding, and assimilating the broad scope and complexities of an architecture description through tabular, structural, behavioral, ontological, pictorial, temporal, graphical, probabilistic, or alternative conceptual means (DODAF 2015).

DODAF, as a methodology, defines a way of representing an enterprise architecture that enables stakeholders to focus on specific areas of interests in the enterprise while retaining sight of the big picture. The DODAF methodology does this by dividing a problem space into manageable pieces that correspond to stakeholder viewpoints, which are further defined as models (Fig. 2).

DODAF organizes models into views (DODAF 2015: 3.1–3.105)

- **Strategic View**: **not part of the traditional DODAF family of views**, but an essential element in understanding the conceptual goals, vision, mandate of the criminal or terrorist networks.
- **Capability View**: describes capability requirements, delivery timing, and deployed capabilities.
- **Operational View**: describes operational scenarios, activities, and requirements that support capabilities.
- **Project View**: describes relationships between operational and capability requirements and various projects to deliver capabilities.
- **Systems View**: models identify and describe system resource flows, organizational activities performed or supported by system functions.

Through the DODAF views, interrelationships between systems/service functions, operational activities, operational nodes, data and information objects, technical standards, rules, policies, timelines, and a number of project and development artifacts are realized.

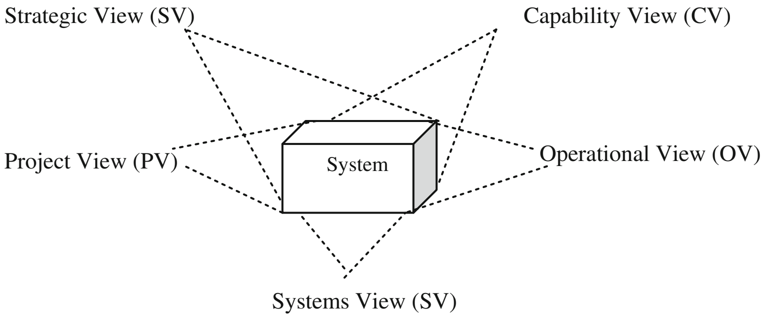


Fig. 2 DODAF views

The Data groups that comprise the development of DODAF views are described in detail in DODAF (2015: 2.5) and includes:

(1) *Performers*. Any entity—human things, automated things, and any assemblage of such things—that performs an activity and provides a capability.
(2) *Resource Flows*. The behavioral and structural representation of the interactions between activities (which are performed by performers) that is both temporal and results in the flow or exchange of things such as information, data, materiel, and performers.
(3) *Information and Data*. Representations (descriptions) of things of interest and necessary for the conduct of activities. Information is the state of a something of interest that is materialized—in any medium or form—and communicated or received.
(4) *Rules*. How rules, standards, agreements, constraints, and regulations are relevant to architectures. A principle or condition that governs behavior; a prescribed guide for conduct or action.
(5) *Capabilities*. The ability to achieve a desired effect under specified standards of performance and specified conditions through combinations of ways (guidance and rules) and means (resources) to perform a specified set of activities.
(6) *Services*. A mechanism to enable access to a set of one or more capabilities. The mechanism is a Performer. The capabilities accessed are resources, that is, information and data, materiel, performers, and geo-political extents.
(7) *Projects*. All forms of planned activities that are responsive to visions, goals, and objectives that aim to change the state of some situation. A temporary endeavor undertaken to create resources or desired effects.
(8) *Organizational Structures*. Representations of the organization types, organizations, and persons in roles that are within the scope of the described architecture.

An example DODAF representation is discussed in Masys and Vallerand (2015).

Through a DODAF representation of a complex organization (such as terrorist or crime syndicate), intelligence agencies can develop a 'holistic' and contextual understanding of the network to support vulnerability analysis.

5 Methodology

In this exploratory work, an integrated methodology for analyzing terrorist and criminal networks for disruption involves the application of network analysis, crime scripting and the development of DODAF products, to support the design of disruption strategies. In this chapter we will explain the methodology within the context of the LeT terrorist network (Subrahmanian et al. 2013) and the Noordin Top's South East Asia terror network (Roberts and Everton 2011).

Data derived from LeT analysis (Subrahmanian et al. 2013) and Norrdin Top analysis (Roberts and Everton 2011) were mapped in accordance with data groups of DODAF. Specific DODAF views were subsequently developed to describe the dynamic process logic models that describe the terrorist case studies.

6 Discussion

Knowledge about the structure and organization of terrorist networks is important for both terrorism investigation and the development of effective strategies to prevent terrorist attacks. The effectiveness of disruption strategies is known to depend on both network topology and network resilience (Duijn et al. 2014: 1) both of which are rooted in the notion of weak ties (Granovetter 1983) which is central to Social Network Analysis (SNA) in showing the linkages between actors. While most research has focused on relational networks based on individuals or small groups of individuals, contextual factors are often crucial for a complete understanding of social phenomenon (Boivin 2014: 49).

In support of security operations, the visual thinking (Strang and Masys 2015) approach of SNA allows the researchers and investigators to discover patterns of interactions among the offenders, including detecting criminal subgroups, central offenders and their roles and discovering patterns of interactions among offenders. Visualization also can provide new insights into network structures for investigators while helping them communicate with others. Effective visualization should be accompanied with a comprehensive and detailed interpretation (Wiil 2011: 93).

Based upon the Noordin Top data (Everton 2011), a network of actors is shown in Fig. 3.

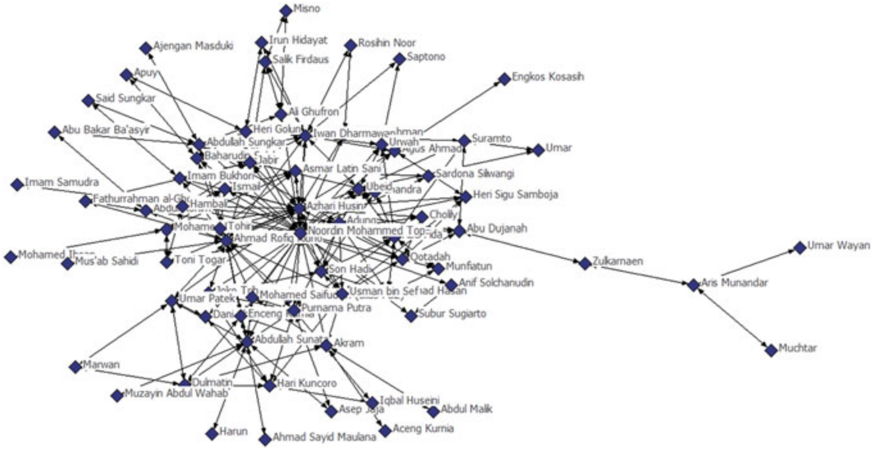


Fig. 3 Noordin Top network (derived from data supplied from Everton 2011)

The network and centrality analysis (Figs. 3 and 4) provides invaluable insights into the network structure highlighting the connectivity across the actors but does not show the context and thereby does not directly support strategic intervention strategies.

The operation of a network is dependent on contextual links. Roberts and Everton (2011) show the value of analyzing a network for context. Figure 5a–f shows a network from 6 perspectives illustrating that all links are not equal and that actors are multiplex.

Whereas the overall network provides a good representation of the connectivity, contextualizing the network along the lines of 'scripts and affiliations' opens the 'operational' blackbox of the terrorist organization. From these network

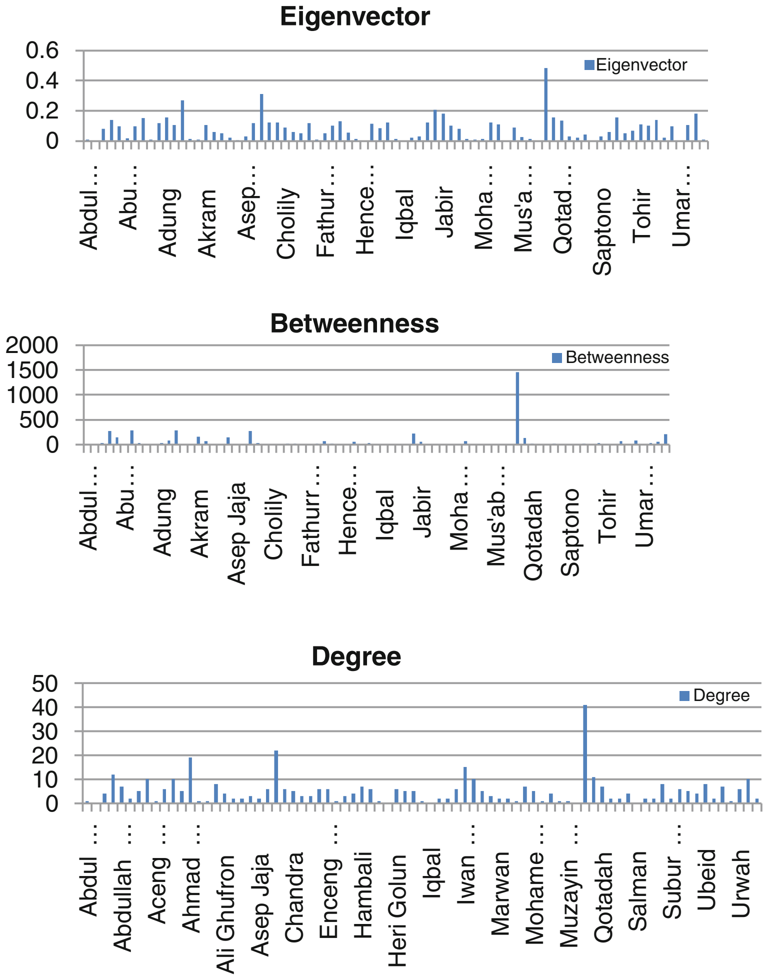


Fig. 4 Centrality analysis results stemming from Noordin Top network (see Fig. 3)

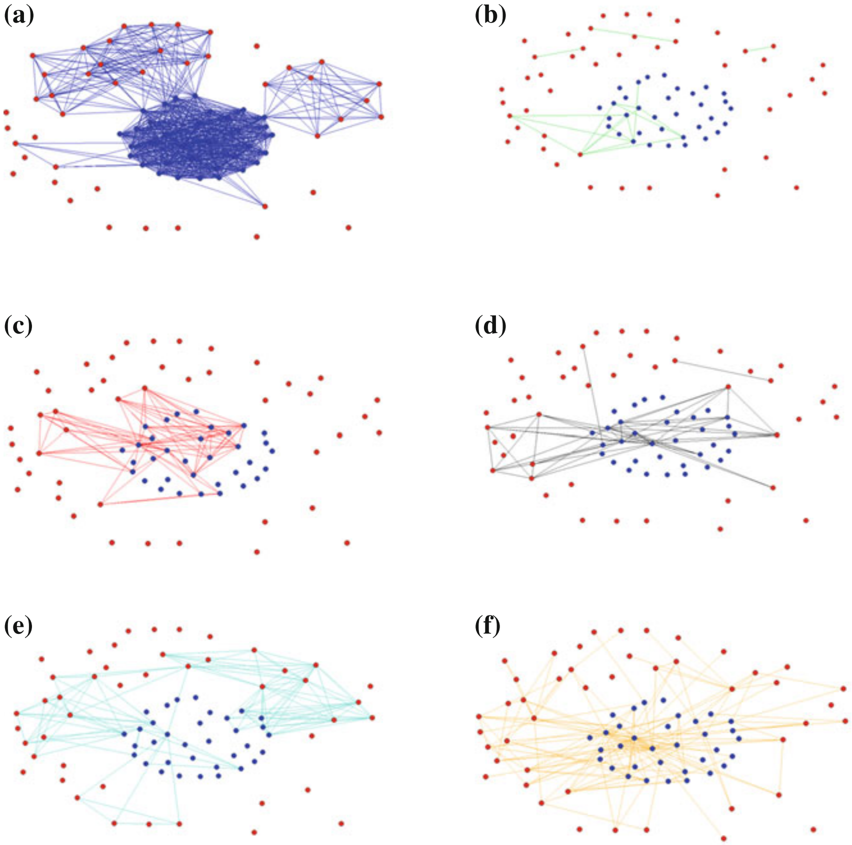


Fig. 5 Noordin Top network analysis (Roberts and Everton 2011). **a** Organizations. **b** Finance. **c** Operations. **d** Logistics. **e** Training. **f** Internal communications

visualizations, the complex interdependencies of these 'dark' network emerges. As described in Duijn et al. (2014: 1) 'Criminal networks are not simply social networks operating in criminal contexts. The covert settings that surround them call for specific interactions and relational features within and beyond the network'. The requirement for contextual understanding and crime scripting of terrorist organizations is certainly recognized. For example, Lindelauf et al. (2011: 62–63) shows that covert network topology '…is strongly resilient against disruption strategies focusing on capturing and isolating highly connected individuals, partly explaining the difficulties in disrupting current terror networks'. In this sense, the crime script is shaped and informed by the network affiliations and operational intent of the terrorist organization.

6.1 Contextual analysis

How we look at the world shapes what we see. The analytics available within SNA provide this window revealing cliques and communities that can represent contextual activity within a network.

As described in Carrington et al. (2005), Easley and Kleinberg (2010), Gunduz-Oguducu and Etaner-Uyar (2014), Masys (2014a), Wiil (2011), analysis of the networks is supported by algorithms that help find equivalences between nodes and thereby support contextualization and interpretation of the networks. Duijn and Klerks (2014: 135) describes how such approaches as block modeling and K-core analysis can support the identification of groups of nodes on the basis of their relational similarities. In so doing, the relations between clusters of nodes are then analyzed to detect general patterns.

From K-Core analysis emerges a methodology to identify subgroups in the overall network: clique analysis. In essence, a clique is a sub-set of a network in which the actors are more closely and intensely tied to one another than they are to other members of the network. How cliques influence the movement of information and resources within and between networks is a key attribute to support the contextual understanding of a terrorist network (Duijn and Klerks 2014: 135–136).

Corman (2006) applies the concept of Activity Focus Networks (AFNs) to terrorist networks, whereby networks are organized around 'activity foci,' defined as 'physical or conceptual entities around which people and their joint activities are organized' to achieve an organizations goals. Corman (2006: 39) argues that '…If we know (or can estimate) the AFN for some terrorist organization, the inputs that activate it, and the organization's capacity for activity, it should be possible to determine combinations of inputs and/or conditions that are maximally dysfunctional for it. Presenting the organization with regular doses of these inputs/ conditions could potentially put it under a great deal of stress, decreasing its effectiveness and generating other desirable outcomes'.

As described in Duijn and Klerks (2014: 129), in addition to exposing the criminal network structure through the social network analysis method, 'crime script analysis' adds insight into the individual positions of actors within a criminal network. Applications of crime scripting to terrorism 'as a dark network' can be justified and supported by similar applications to organized crime 'dark networks'. For example, Bruinsma and Bernasco (2004) described in Duijn and Klerks (2014: 129) combined crime script analysis and social network analysis to describe the flexibility within the criminal markets of heroin trade, trafficking in women and car theft. They found some evidence that the structure of criminal networks was shaped according to the features of the criminal activities. Crime script analysis, Fig. 6, is thereby a game changing method that supports network analysis.

It is recognized in the research on covert networks that a focus on highly connected individuals for disruption without understanding the context will not address the resilience inherent within the network. Lindelauf et al. (2011: 61) describes how these covert networks are well suited against such targeted attacks as

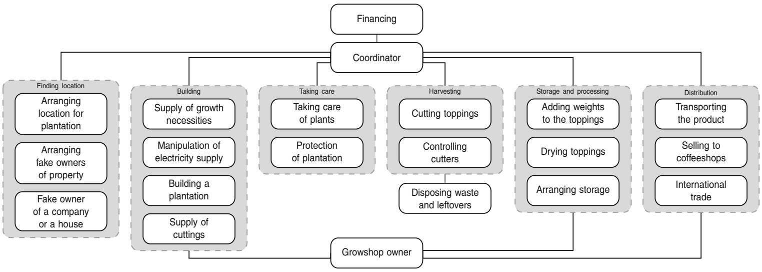


Fig. 6 Crime script of cannabis cultivation (Emmet and Broers 2009; Morselli 2001; Spapens et al. 2007: from Duijn and Klerks 2014: 130)

shown by the resilience properties of secrecy versus information balanced networks. This provides an explanation of the survival of global terrorist networks and food for thought on Counter-terrorism strategy policy.

Context is key to supporting disruption strategies. Broker nodes emerge as key attributes in many crime script scenarios (financial, drug trafficking). Knowledge of these and subsequent targeting may degrade the function of the network. At the least such a disruption would cause the network to react. Such intervention probing can reveal much about the structure and dynamics of the network. Bakker et al. (2012) describe how networks specializing in recruitment appear to be more robust and resilient to the removal of even multiple nodes. As Bakker et al. (2012) confirm, '…much work remains to be done on how networks replace nodes, re-establish links or re-route flows of information and/or resources through other nodes; so, it is difficult to predict how effective the removal of nodes would be over time' (Bakker et al. 2012: 56–7). Leuprecht and Hall (2014: 115–116) argues that 'the possibility that a network's function and structure are related is a promising step towards a more nuanced strategy to contain and deter such networks: not all terror networks are alike. This is a significant empirical finding for counter-errorism. Knowing the function of a network makes it possible to counter it by detecting and debilitating its nodes. Conversely, knowing the structure of a network makes it possible to surmise its purpose'.

6.2 DODAF and SNA: Topology and Functionality

As described in Duijn et al. (2014: 3), the most central actor isn't necessarily the network member with the most leadership potential. For instance, they found that in networks where leadership and centrality are fulfilled by different actors, targeting the central node would not necessarily lead to a downfall of the network and that a targeted leader is not necessarily replaced by the most central actor.

Context is key. Does the actor have a strategic, operational or tactical role in the network?

Roberts and Everton (2011) emphasizes that features of network topology also interact with individual-level factors. Therefore qualities of individual actors (e.g. skills, expertise, information and knowledge) cannot be ignored in understanding the complex dynamics within criminal networks.

These studies illustrate that although the centrality approach is a useful approach to identify potentially 'critical' actors for criminal network disruption, an additional qualitative assessment on the individual level is essential for understanding the effects of network disruption (Duijn et al. 2014: 3).

Using DODAF modeling to support crime script analysis, we begin to understand strategies to support counter terrorism ops.

Roberts and Everton (2011) emphasize this:

> … identifying high-value targets is an important option to consider, but we want to encourage analysts to consider the wide variety of SNA metrics available, many of which we believe will prove useful in combating terrorist networks. This is not to say that we should abandon the use of centrality metrics. Indeed, we employ them extensively in our analysis below. However, we use them in conjunction with other algorithms (e.g., blockmodeling, centralization, density, QAP correlation) and for more than simply identifying high-value targets. What we are suggesting, in other words, is that analysts view centrality metrics as one set of SNA algorithms among many that can be used to help flesh out a range of strategic options. For example, at the individual level, centrality (e.g., degree, closeness, betweenness) and brokerage (e.g., structural holes, cutpoints, and Gould and Fernandez brokerage scores) algorithms can be used to identify key and peripheral players within the network, while blockmodel (e.g., structural and regular equivalence) and cohesion (e.g., cliques, components, k-cores) algorithms can be used to identify subgroups that could possibly be set at odds with one another.

With this in mind, the application of DODAF supports the need argued by Roberts and Everton (2011: 7) '…to combat terrorist networks, analysts need to collect multi-relational (i.e., multiplex) data, be explicit about the various types of ties they code and examine, analyze data at multiple levels of analysis (i.e., individual, subgroup, and organizational/institutional), and use the wide variety of SNA algorithms available to them'.

A network diagram is insufficient to support understanding regarding the dynamics of a terrorist network. Using data of LeT and Noordin Top, an operational view was developed through the application of DODAF. This afforded an understanding of the crime script associated with the terrorist operations. The Operational Views examines the activities, performers and resources. In so doing it can reveal materiel, systems, and services—as constraints. An activity consumes resources to produce resources. Performers, themselves resources, follow guidance, rules, and standards to carry out activities. Activities are carried out under conditions that affect their performance (secrecy and impact). Coupled with affiliation networks (Roberts and Everton 2011) and network analytics, greater resolution of the network is created. By incorporating a variety of DODAF views, it is suggested that disruption strategies can be developed that consider the contextual operational understanding of the terrorist network described through the 'crime script'. Mapping such affiliation networks (Fig. 5a–f) to the DODAF crime scripts facilitates development of disruption strategies.

Examining the LeT network (Subrahmanian et al. 2013) and the Mumbia bombing, an OV (see Table 1 for a listing of OV views) was developed from the data illustrating the strategic, operational and tactical operations. As shown in Table 1, different views afforded by DODAF reveals different perspectives and context associated with the network. In this way the combination provides a more holistic view and thereby facilitates a greater informed targeting analysis.

Figures 7 and 8 are OV-6c and OV-1 derived from data provided (Subrahmanian et al. 2013). Insights from SNA can be derived from consolidating both the OV and SNA plots. This crime scripting utilizing DODAF helps to contextualize the network analysis. Everton (2011) describes how different views (network affiliations) reveal different context.

Mapping affiliation networks developed in Fig. 5a–f to the OV 6c and OV-1 helps to better understand how terrorist operations are strategically, operationally and tactically conducted and how organizational networks become entangled in the crime scripting. What this suggests is that disruption strategies developed through SNA, DODAF and crime scripting are better informed.

For example in recruiting and radicalization, Masys (2014b) describes the process of radicalization through the lens of systems theory and actor network theory. Understanding the underlying processes and actors supporting the process of radicalization, vulnerabilities can be revealed and intervention strategies can be developed. Figure 9 shows a 'rich picture' (Checkland 1981) developed in support of conceptual modeling on radicalization and recruitment (Masys 2014b). From the Actor Network Theory (ANT) perspective, the path to radicalization through low-risk/low-cost actors is fostered through the process of problematization,

Table 1 Operational views (DODAF 2015)

DODAF view	Description
OV-1: operational concept	Presents the concepts of operation of a described architecture
OV-2: organizations and resources	Presents resources that are used by organizational performers
OV-3: organizations, activities, and resources	Presents resources that are consumed and produced by activities performed by organizational performers
OV-4: organizational relationships	Presents the composition and relationships among organizational performers
OV-5a: operational activity hierarchy	Presents the hierarchical structure of organizational activities
OV-5b: operational activities	Presents activities performed by organizational performers to consume and produce resources
OV-6a: operational rules	Presents rules that constrain organizational activities
OV-6b: operational state transitions	Presents the states of resources consumed and produced by activities performed by organizational performers
OV-6c: operational activity sequences	Presents sequences of activities performed by organizational performers

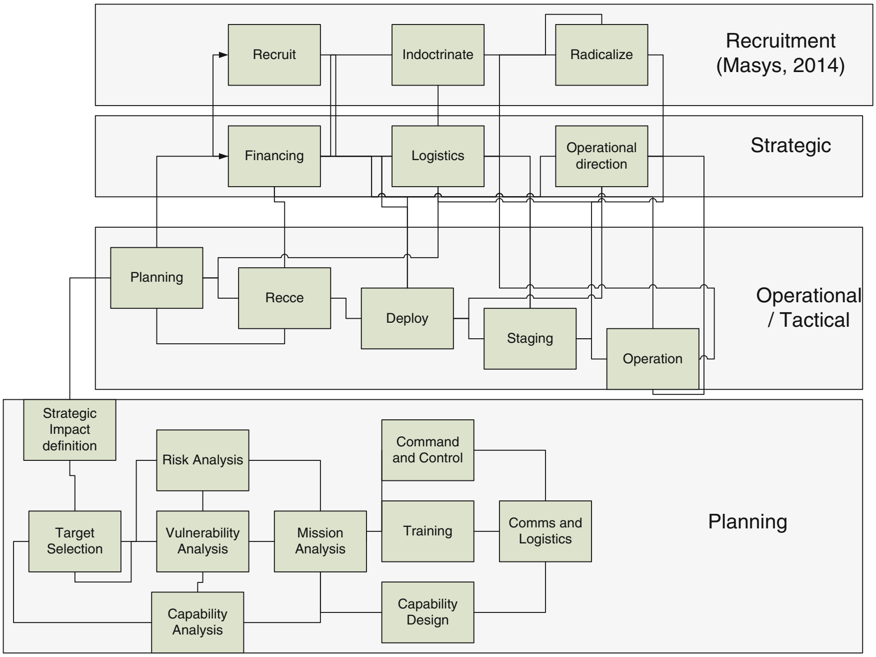


Fig. 7 OV-6c functional operational processes of LeT

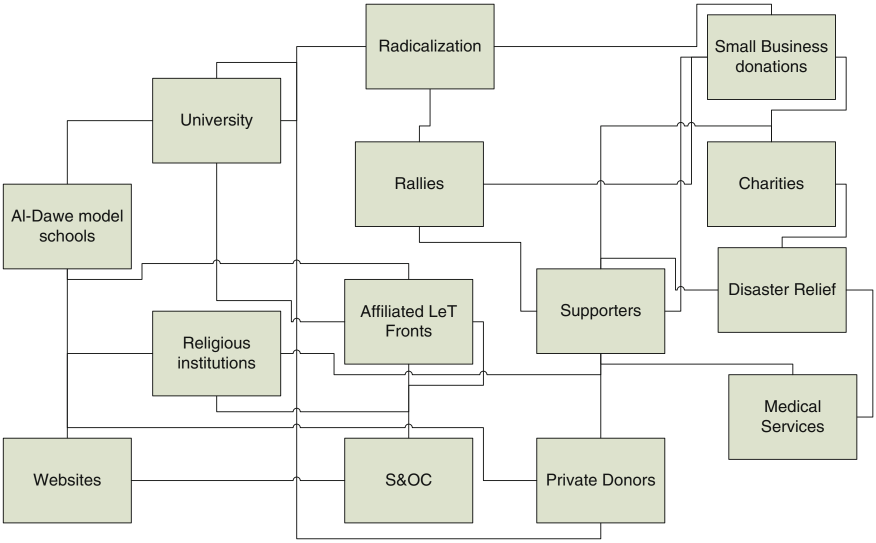


Fig. 8 OV-1 functional relationality of terrorist financing for LeT

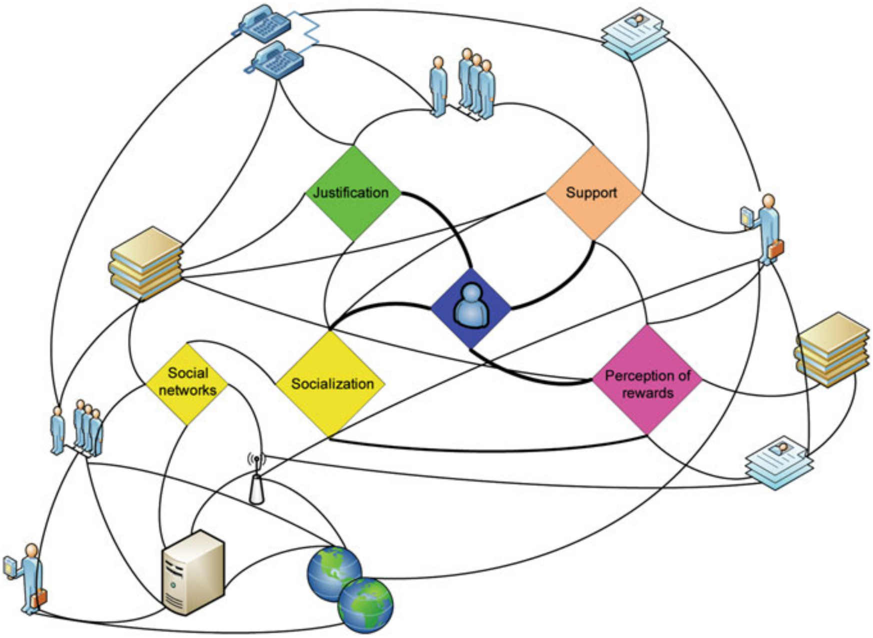


Fig. 9 OV-1 conceptual mapping (rich picture) of translation process (Masys 2014b: 57)

interessement, enrolment and mobilization on the actor. The high level factors of socialization, perception of rewards, support and justification figure prominently in this process.

Amongst the heterogeneous elements that make up the actor network, power emerges, circulates and reifies within the translation process. Socialization, perception of rewards, justification and support thereby become inter-connected and are fluid within the translation process as depicted in Fig. 9, a rich picture that becomes the OV-1.

This contextual understanding can help shape intervention strategies for countering violent extremism. There are challenges associated with such analysis stemming from the uncertainty and ambiguity of the data associated with the dark network mapping. Gaps exist and assumptions must be made. Rhodes and Keefe (2007) present an approach to help 'fill the gaps and connect the dots' that can support this CTAF analysis. Using a Bayesian approach, attribute data such as age, gender, religious persuasion, social background, job function can be used to infer the likelihood of links between individuals. The power of the Bayesian method resides in its ability to take data that, of itself, is weakly predictive of interaction and to combine it with other data to systematically increase or decrease confidence in the likelihood of there being a social tie (Rhodes and Keefe 2007: 1606).

The objective is to predict on the basis of attribute data, where the other individuals might fit into this core network. The procedure for the calculation is presented in Rhodes and Keefe (2007) (Rhodes 2011: 164).

6.3 Conclusion

Network analysis continues to offer valuable insight into the structure and organization of terrorist and criminal networks. Contextualizing the network through crime scripting facilitated through DODAF views, supports analysis and formulation of disruption strategies. Knowledge about the architectural complexity of dark networks is a step forward in understanding the underlying dynamics. DODAF provides this contextual lens to support crime mapping and SNA of terrorist organizations.

The complexity of terrorist networks requires a crime script at different levels. Here we introduced CTAF as a methodology to support Counter-terrorism operations. When linked with SNA and crime scripting, CTAF provides greater contextual understanding of terrorist networks thereby supporting targeting and disruption strategies.

References

Aghakhani S, Dawoud K, Alhajj R, Rokne J (2011) A global measure for estimating the degree of organization and effectiveness of individual actors with application to terrorist networks. In: Wiil UK (ed) Counterterrorism and open source intelligence. Springer, Wien, New York, pp 189–222

Bakker RM, Raab J, Milward HB (2012) A preliminary theory of dark network resilience. J Policy Anal Manage 31:33–62

Boivin R (2014) Macrosocial network analysis: the case of transnational drug trafficking. In: Masys AJ (ed) Networks and network analysis for defence and security. Springer, Berlin

Bruinsma G, Bernasco W (2004) Criminal groups and transnational illegal markets. Crime, Law, Soc Change 41:79–94

Carrington PJ, Scott J, Wasserman S (eds) (2005) Models and methods in social network analysis. Cambridge University Press, Cambridge

Checkland P (1981) Systems thinking, systems practice. Wiley, Chichester

Chiu Y-N, Leclerc B, Townsley M (2011) Crime script analysis of drug manufacturing in clandestine laboratories. Br J Criminol 51:355–374

Corman S (2006) Using activity focus networks to pressure terrorist organizations. Comput Math Organiz Theor 12:35–49

DODAF (2015) DODAF V 2.0. volume II: architectural data and models. Available at: http://dodcio.defense.gov/Portals/0/Documents/DODAF2/DoDAF%20v2.02%20Chg%201%20Vol%20II%20Final%202015-01-19.pdf. Accessed 11 Oct 2015

Duijn PAC, Klerks PPHM (2014) Social network analysis applied to criminal networks: recent developments in dutch law enforcement. In: Masys AJ (ed) Networks and network analysis for defence and security. Springer, Berlin

Duijn PAC, Kashirin V, Sloot PMA (2014) The relative ineffectiveness of criminal network disruption. Scientific reports|4: 4238 available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3937802/pdf/srep04238.pdf

Easley D, Kleinberg J (2010) Networks, crowds and markets: reasoning about a highly connected world. Cambridge University Press, Cambridge

Everton SF (2011) Disrupting dark networks. Cambridge University Press, Cambridge

Global Terrorism Index (2014) http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%20Report%202014_0.pdf

Granovetter M (1983) The strength of weak ties: a network theory revisited. Sociol Theor 1:201–233

Gunduz-Oguducu S, Etaner-Uyar AS (2014) Social networks: analysis and case studies. Springer, Berlin

Leclerc B (2014) Script analysis for crime controllers: extending the reach of situational crime prevention. In: Caneppele S, Caldroni F (eds) Organized crime, corruption and crime prevention. Springer Publishing, Berlin

Leuprecht C, Hall K (2014) Why terror networks are dissimilar: how structure relates to function. In: Masys AJ (ed) Networks and network analysis for defence and security. Springer Publishing, Berlin

Levi M, Maguire M (2004) Reducing and preventing organised crime: an evidence-based critique. Crime, Law Soc Change 41:397–469

Lindelauf R, Borm P, Hamers H (2011) Understanding terrorist network topologies and their resilience against disruption. In: Wiil UK (ed) Counterterrorism and open source intelligence. Springer, Berlin

Masys AJ (ed) (2014a) Networks and network analysis for defence and security. Springer Publishing, Berlin

Masys AJ (2014b) Radicalization and recruitment: a systems approach to understanding violent extremism. Int J Syst Soc 1(2):51–65

Masys AJ, Vallerand A (2015) Major event security planning: secure by design—through the strategic use of integrated modeling and simulation. M&S J

Rhodes CJ (2011) The use of open source intelligence in the construction of covert social networks. In: Wiil U (ed) Counterterrorism and open source intelligence. Springer, Berlin

Rhodes CJ, Keefe EMJ (2007) Social network topology: a Bayesian approach. J Op Res Soc 58:1605–1611

Roberts N, Everton SF (2011) Strategies for combating dark networks. J Soc Struct 12(2). http://www.cmu.edu/joss/content/articles/volume12//RobertsEverton.pdf

Strang S, Masys AJ (2015) Visual thinking for intelligence analysis. In: Masys AJ (ed) Applications of systems thinking and soft operations research in managing complexity. Springer Publishing, Berlin

Subrahmanian VS, Mannes A, Siliva A, Shakarian J, Dickerson JP (2013) Computational analysis of terrorist groups: Lashkar-e-Taiba. Springer Publishing, Berlin

The Economist (2015) http://www.economist.com/news/leaders/21646750-though-islamic-state-still-spreading-terror-its-weaknesses-are-becoming-apparent

Wiil UK (ed) (2011) Counterterrorism and open source intelligence. Springer Publishing, Berlin

Computing in Compromised Environments: Beyond the Castle Model of Cyber-Security

David Skillicorn, Christian Leuprecht and Victoria Tait

Abstract The predominant metaphor for secure computing today is defence in depth: higher, better layers of walls. This article explains why that approach is as outmoded for cybersecurity today as it became for physical security centuries ago. Three forces are undermining the castle model as a practical security solution. First, organizations themselves tear down their walls and make their gateways more porous because it pays off in terms of better agility and responsiveness—they can do more, faster and better. Second, technological developments increasingly destroy walls from the outside as computation becomes cheaper for attackers, and the implementation of virtual walls and gateways becomes more complex, and so contains more vulnerabilities to be exploited by the clever and unscrupulous. Third, changes in the way humans and technology interact, exemplified (but not limited to) the Millennial generation, blur and dissolve the concepts of inside and outside, so that distinctions become invisible, or even unwanted, and boundaries become annoyances to be circumvented. A new approach to cybersecurity is needed: Organizations and individuals need to get used to operating in compromised environments. The article's conclusion operationalize this strategy in terms of a paradigm shift away from a Castle Model and towards a more nuanced form of computation and data assurance.

Keywords Cyberdefense · Security · Organizational boundaries · Millennials · Generational differences · Compromised environments

D. Skillicorn
Queens University, Kingston, Canada

C. Leuprecht (✉)
Royal Military College of Canada, Kingston, Canada
e-mail: christian.leuprecht@rmc.ca

V. Tait
Carleton University, Ottawa, Canada

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_12

1 Introduction

Walls have a dubious history as tools of defence. The Roman Empire disintegrated despite Hadrian's Wall. The Great Wall of China became irrelevant once China's elite, confronting a peasant rebellion, invited in those same Mongols the Wall had been meant to keep out. Its modern incarnation, the Great Firewall, has Chinese spoofing IP addresses to circumvent it. The Maginot line failed to keep the Wehrmacht out of France. The Berlin Wall could not isolate East Germans from the lure of a better life, and was eventually dismantled. The border between the United States and Mexico remains porous, various barriers notwithstanding. Fencing has not prevented migrants from swarming Ceuta and Melilla. The "Castle Model" of cybersecurity is as alluring as these physical defences but, as we shall show, creates an equally false sense of security.

This article problematizes the relationship between risk and security in cyberspace. Hitherto cybersecurity has been taken as a "given," a banal fact of the digital world in which we live. By contrast, understood as a social process, cybersecurity as a mundane vernacular becomes untenable: operationally, conceptually, and theoretically. That cyberspace is yet another example of the way the success of modernity is changing society is uncontroversial; not so the transformation of order in the form of unseen consequences of cyberspace where our institutional resources are unable to cope. This article posits cyberspace as yet another example where the success of modernization is creating problems it is unprepared to solve with present-day institutions. It shows how uncertainties in cyberspace are manufactured, and the inability to control them, and the feedback loops and consequences they engender.

The imbrication of the digital and materials worlds is well established (Sassen 2002). So is the Internet as a productive system (Foucault 1991, 1998) that transforms ordinary citizens (Bauman and Lyon 2013). It is a socializing agent that creates citizens and consumers through a process of discovery and participation: it allows adolescents to share, discuss, influence and learn interactively from each other and from the medium. In cyberspace, activities such as communication, commerce, and entertainment, are conducted, mediated, and learned socially in a way that differs fundamentally from physical space (Lee and Conroy 2003: 1709). The "digital drift" that follows from the individualization that cyberspace enables "individuals to both 'embed' and 'disembed themselves in a variety of criminal activities and lifestyles off- as well as online. [These changes] impact upon the level of individual commitment to criminal activities and lifestyles as well as upon the degree and forms of interdependence and reciprocity implicated in the accomplishment of crime" (Goldsmith and Brewer 2015: 2). The micro-social dimensions of criminality, especially those mediated by the Internet, thus warrant closer attention (Resnyasnsky et al. 2012). The article's preoccupation with cybersecurity is one corollary of the qualitative change in cybercriminality.

In cyberspace individuals do not merely observe and model routes of data production; they engage in a process of discovery and participation that gives rise to "technologically mediated sociality" (Tufekci 2008: 21; Pariser 2012). Individuals divulge information about themselves in ways and to an extent that is quite unprecedented in physical space, they play with and within the boundaries of the software, react to and resist the impulsions written into the codes, set up revelatory profiles, hold back or give info (Beer 2009: 998, 2014). In fact, cyberspace's "impotentiality" encourages citizens to do anything while diminishing the ability "not to" do anything and everything (Agamben 1999).

Security in the physical world involves social processes. The sociology of surveillance has long shown the same to hold for security in the digital age. Yet, neither surveillance studies nor critical theory has explicitly pondered the social processes that cause an individual to be in/secure in cyberspace, nor the implications that follow. Individuals enter, explore, exploit, and exit cybserspace. It is their nascent, emergent, tentative behavior, and the social processes that ensue, that generates cyberrisk in the first place. Luhmann, Giddens, and Habermas are renowned for observing how risk is related to decision-making, but those decisions are also creating largely unintended consequences for others (Leydesdorff 2010). By virtue of its interconnectivity, cyberspace is the prime example where deciders and those who are affected by the consequences have little ability to participate in decision-making. Once user, interface, executables, platforms are situated in the cyber-habitus, it becomes clear that the current paradigm of cybersecurity and its provision is fundamentally flawed.

Organizations with security concerns normally frame the issue as a dichotomy: "inside" versus "outside". What happens inside the organization is permissible; what happens outside is considered to be, at least potentially, harmful or dangerous. This framing applies to countries and their governments [see, for instance, a recent review of US cybersecurity policy by Harknett and Stever (2011)], to government departments, including the military and security components, to businesses, to other kinds of organizations, and even to households, where land is delineated by property lines, and houses by lockable doors and windows. The difference between "inside" and "outside" is a delineation that defines the two sides. No organization can exist as an island. Boundaries must inevitably have gateways that permit resources and information to flow in and out. This separation into inside and outside can also exist recursively within the organization. For example, departments within an organization can have their own "inside" and regard (at least in some sense) the rest of the organization as "outside". This explains, for example, the persistent difficulty of sharing intelligence among organizations within the same government.

This metaphor of "inside" and "outside"—euphemistically known as defence in depth—is better called the Castle Model (Frincke and Bishop 2004), since it replicates the mindset of the medieval castle: strong (often layered) walls preserving the integrity of the inside against any form of attack from the outside—and the ability to impose strict controls over movement in and out (but with a curious blind spot to movements within). As in physical castles, walls in cyberspace are costly to build and impede the movement of digital goods, services, and information between the inside and the outside. When these "castles" fail to nest properly, difficult issues present themselves that hint at the fraying of this view of the world. Businesses were once contained inside national borders; the rise of multinational corporations, with their own boundaries that intersect national borders, creates difficult issues that reveal themselves in, for example, the problems that national governments have collecting taxes they are owed.

Quigley and Roy link the approach to cyber security and typical reactions to a security breach to cultural theory. They argue that governments favour a "hierarchist" approach to security. This method emphasizes the importance of structure, rules, and fairness. Any departure from the hierarchy and rules signifies a risk that may not be overcome if members of the hierarchy have inadequate training or skills (Quigley and Roy 2012). While the hierarchic structure can be beneficial for organization, it leaves little margin for error. Additionally, the government's hierarchist approach focuses on control; this approach can be intimidating for private sector partners. Were a cyber security crisis to occur, governments require flexibility and partners.

Although all boundaries differentiate inside and outside, they can make this differentiation in multiple ways. Organizations have boundaries in at least three important domains:

The first is physical—there are physical or geographical spaces that are defined to be inside the organization. When the organization is a country, this is its territory; when it is a business, this is its workplace (factories, offices, warehouses, and retail space). Boundaries that separate inside and outside in this domain are usually obvious: walls and fences; and gateways and doors to pass through them.

The second domain is temporal—there are times that, at least for businesses, are defined to be inside. We call them the working day. Boundaries in this domain are less obvious, but they are there nevertheless. In some businesses, employees must clock on and off; in others the maintenance of these boundaries is a management task, and employees are expected to seek permission when they will not be "inside" during the normal, expected times.

The third domain is the online world—there are computational and network resources that are considered as inside the organization; and a much larger set that is considered outside. The boundaries in this case are a set of electronic and computational wall technologies that are designed to stop data from moving in and out, except as allowed. The gateways now become more distributed and harder to see, which raises new issues.

Some of these wall technologies are:

- Antivirus software that examines incoming email and web traffic for the signatures of known attacks.
- Firewalls that embody rules about what other kinds of traffic is allowed in and out of the organizational network and individual systems.
- Anti-spam software that examines incoming email for messages that are not real communications.
- Authentication mechanisms such as passwords that allow only approved users to access the network and systems.
- Exfiltration detectors that examine outgoing data and block any (usually documents) that are intended to remain inside the network.

Authentication mechanisms sufficed for standalone systems. These other virtual wall technologies are the response to systems that are connected to the Internet; consequently, their internal content is potentially accessible to anyone on the planet. Even organizations that are not connected to the Internet, for example militaries and security and intelligence organizations that run their own air-gapped "closed" networks, have been forced to admit that they cannot really consider themselves as separate from the larger world. For example, ubiquitous cameras on laptops mean that data can be passed by pointing the camera of a computer on an outside network at the screen of a computer on an inside network; ubiquitous microphones mean that a computer on an outside network can listen to sounds made by a computer on an inside network (even at frequencies inaudible to humans).

Boundaries, and so the preservation of the concepts of inside and outside, have been dissolving under three main forces:

- Strong incentives to reduce boundaries because of the opportunities this creates for agile response to the environment and streamlined access from the outside; and the cost of constructing, operating, and maintaining boundaries;
- Technological changes to the way organizations structure their computational resources that make boundaries increasingly porous; and
- Changing human culture, captured most strongly in the so-called Millennial generation, for which boundaries are becoming irrelevant.

2 Organizations Are Tearing Down Walls from the Inside

The first driver of change is the opportunities that having weaker boundaries create in a connected world, and the costs of putting boundaries in place and operating them.

Removing or weakening boundaries allows more flexible travel and use of human capital in the physical world, and new levels of sophistication in acquisition of information and coordination in the online world. For example, the Schengen area in Europe allows unfettered movement across national borders, making it easier for business interaction and tourism. More flexible working hours encourage greater workforce participation. Allowing employees to access email at home has ushered in a new level of business responsiveness. Making it possible for citizens to access government services from their homes, rather than having to visit a government office, has streamlined service delivery. Reducing or weakening boundaries has considerable upsides: flexibility, greater workforce participation, and responsiveness.

Also, creating and enforcing strong boundaries imposes considerable costs and delays. These boundaries have to be built and operated, a cost that is approximately proportional to how robust and secure they are. They also impose delays and costs whenever something has to pass across them. National borders create the need for visa and passport mechanisms, lines at borders to verify who may cross, and civil servants to administer the process. Security for buildings requires locks and keys, CCTV, and security guards to control entry and egress. Fixed working hours require time clocks (and those who check them) or management's attention to tardiness.

Erasing such boundaries reduces the marginal costs they impose. As organizations face a more competitive world, where expectations of productivity, efficiency, performance and responsiveness increase, and where overheads continue to be squeezed, it is unsurprising that they feel pressure to reduce transaction costs by reducing boundaries (Pew 2010: 23). Many organizations have yet to come to grips with the impact this has on their conception of inside and outside, and the ensuing security implications.

3 Technological Developments Are Destroying Walls from the Outside

The second driver of change is the increasing difficulty, even impossibility, of providing strong boundaries because of technological change.

In the physical world, the reduced costs of transport (private places, unmanned aerial vehicles, small submersibles) and the increased ease of forging documents (physical or electronic) is making borders more porous. The difficulty that the U.S. has in interdicting drug shipments and illegal immigration, despite having a strong border-security regime and having put considerable resources into it, illustrates this development. In the context of building security, keys are easy to copy, and even "high-end" technologies such as fingerprint readers and iris scanners are relatively easy to spoof.

In the cybersecurity domain, the virtual wall technologies discussed above are all becoming increasingly porous (McDougal 2009). Quigley and Roy found that these porous networks are allowing cybersecurity threats to flourish. Websense Security Labs found that over the span of a half year threatening websites had increased by an overwhelming 233 %. Additionally, there was a more narrowed focus on data. Of the threats recorded, 37 % involved stealing data (Quigley and Roy 2012). These statistics from 2009 show that there is a growing, threatening presence in the cyber sphere, and frequent news stories indicate how these figures are increasing as technology advances.

When passwords provided access to a single system from a dedicated, connected device, it was easy to protect them. When passwords must necessarily pass over public networks, they cannot be robustly protected, even though they are encrypted. Standard attacks require only that every possible string (shorter than a given length) be encrypted using one of only a few standard algorithms and compared to the encrypted password to discover what the plaintext password is. The computational requirements to do this are, by today's standards, modest and can be rented from grid service providers for a few dollars. The only defence is to make passwords long, so that many potential strings must be encrypted by the attacker—but even a 15-character password is only a mild impediment, and humans begin to struggle to remember strings as long as this. New methods of authentication have proven difficult to build and operate reliably: multifactor authentication can be awkward to use, and biometric authenticators easy to spoof.

Virtual wall technologies also have two major weaknesses: (i) it can be hard to identify where the walls actually are; and (ii) the hardware and software that implements the virtual wall is almost invariably not built by the organization using it; rather, it is bought off the shelf. Paradoxically, then, technology meant to protect actually introduces new vulnerabilities.

The first weakness means that it is hard to know where a virtual wall is needed, and makes it easy to miss places where a wall might be necessary. For example, virtual private networks allow employees to use the organizational network from home as if they were physically connected to it. However, the connection between the home computer and the organizational network is now a vulnerability, even if it is encrypted (as the recent Heartbleed vulnerability dramatically showed) (CVE 2013); and the home computer has become, in practice, a part of the organizational network, together with any virus and malware infections it may have previously acquired. Exfiltration detectors can be defeated by first moving a document to a home computer and disseminating it from there. Other tools such as Microsoft's Remote Desktop allow similar functionality with even less protection. Despite the vulnerabilities created by the ability to connect remotely, many organizations feel compelled to allow telecommuting, and want their employees to be available 24 × 7 because it allows organizational responsiveness that increases the bottom line. As far as we are aware, there are no standard products that allow a remote computer to be incorporated into an organizational network in this way while preserving the full security that a computer physically located on the network would have.

The recent trend towards using clouds for storage and computation introduce similar vulnerabilities. If organizational data is stored in a cloud, that data is no longer clearly inside the organization. The process of transferring it from organizational systems to the cloud creates a potentially vulnerable channel; the data held by the cloud may be vulnerable to access by others, even if it is encrypted; and the data becomes a kind of hostage to the hosting organization. For example, a failure of their systems or an injunction served on them for an unrelated matter may prevent continuing access to the data in a timely fashion.

A somewhat similar vulnerability comes from allowing other organizations to access a given organization's network. There are strong incentives for this: business-to-business connectivity allows collaborative work to happen smoothly; just-in-time component delivery requires a supplier to be aware of not only how much of a component is held by the consumer, in real time, but also the rate at which it is being consumed, so that the optimal time for the next delivery can be planned sufficiently far in advance. A major data breach of the retail chain Target occurred at the end of 2013; the attack came via access granted to an HVAC supplier. Organizations that implement strong security themselves can be vulnerable because of the weaker security of these partner organizations that they regard as separate (outside), but are actually salients of the more secure organization.

Another category of vulnerability comes from the evolution of web browsers as tools, not just for the consumption of static information, but as portals for two-way information flow, and often control of other systems. The problem here is that all traffic involving a web browser travels over the same port: port 80. As a result, all sorts of different traffic, innocuous and potentially dangerous, flows over a single channel. Blocking it would cut off even the simplest web browsing, so it is almost invariably left unblocked. It is extremely difficult to parse the traffic stream that passes through this channel to block some kinds of traffic while allowing others. This is an extremely difficult task, and the bar is constantly raised as more and more services are piggybacked on the ubiquitous browser-server mechanism.

Nor are the cyber and physical worlds decoupled. In 2008, U.S. military networks were successfully infiltrated by a worm on a USB device which had been dropped in a military parking lot in the Middle East; the U.S. Department of Homeland Security carried out an experiment where they dropped USB devices in various parking lots in the U.S. and found that more than 60 % of them were picked up and plugged into computers (Bloomberg 2011). The walls of an organization's network may be as simple as the USB connectors on its systems.

Another vulnerability of the castle model of security is that it distracts attention from what is happening *inside* the walls. A major weakness is the ability of insiders to carry out attacks from within the organization. This is a particular problem, even for organizations with high levels of security, because of the prevalence of contractors who are treated as insiders, but may not have the organization's interests at heart. They do not usually have the same degree of loyalty because they are not subject to the same amount of hostage capital as permanent employees and may, therefore, have an incentive to prize individual gain in the short-term over long-term payoff for the organization as a whole. They may also not have been vetted to the same level as mainstream employees. Edward Snowden stands out as the prime example, partly the National Security Administration (NSA) for which he was a contractor is among the most secure in the world. Bradley Manning, a former uniformed member of the US Department of Defence (DOD) is another high-profile example. Why the two most prominent examples are both American, and why they both came from the US national security apparatus, is an interesting puzzle of its own.

The technologies that implement the virtual wall technologies are themselves a source of vulnerability. Very few organizations implement these technologies themselves. Indeed, to do so would require building their own hardware, and then a considerable amount of software. Instead, most organizations use off-the-shelf hardware and software systems that they configure by defining sets of rules of what is allowed and forbidden. Even if these rules are correct, the organization cannot know if there is a vulnerability embedded in the system that applies the rules. Worse still, some of these technologies have a mechanism that exists to allow them to be updated remotely. The organization using them may not even be aware that this mechanism exists and, because it is built into the wall, other wall technologies may not notice it.

4 Changes in Human Interaction Are Blurring the Distinction Between Inside and Outside

The third driver of change is the new attitudes to connectedness that have developed in a population that has discovered the Internet and cheap network access, and even more strongly in the generational cohort that has grown up with it. The so-called Millennials, the generation born between, roughly, 1984 and 2004, are now beginning to become the majority of the workforce, as Baby Boomers retire. These "digital natives" did not discover and learn network technology: it has been a ubiquitous background to their lives while growing up. Their attitudes to technology, work and organizations are having an impact on how organizations conceive themselves that is at least as significant as the effects of technology per se. Many of their attitudes are also held by earlier generational cohorts, but with lower intensity. Previous generations also use technology less fluently, and, therefore, with more variability.

Some of the characteristics associated with Millennials are:

- They expect technical innovation as a matter of course; they have seen it happening steadily throughout their lives, they expect it to continue, and a significant portion feel a need to be on the forefront of technical change. Whereas previous generational cohorts included "early adopters", Millennials *are* early adopters (Deloitte 2012).
- They depend on technology. Millennials are used to a world in which a personal communication device is always within reach, even when sleeping. This device can connect them to other individuals in their personal peer groups, and to the informational content of the entire Internet instantaneously and in an almost unlimited way. They expect connectivity everywhere, on public transport, on aircraft, in tunnels, and in meetings. Their sense of physical space is weakened by virtue of the fact that they carry a substantial part of their environment with them (Hershatter and Epstein 2010).
- They interface differently to the world than previous cohorts, both in terms of perception and interaction. Their approach to knowledge tends towards just-in-time information gathering, rather than just-in-case learning. This poses challenges for the educational establishment; it also means that Millennials tend not to plan, even for events as simple as getting together with friends, converging on time and place in real time. Similarly, their relationships are simultaneously tighter and looser than previous generational cohorts (Pew 2010: 9): tighter because it is easy to remain connected, in a superficial way, to many people (it is hard to imagine Millennials coming to a high school reunion to find out how their classmates have turned out—they will already know, at least to some extent); but looser because, even when they are physically together, some part of their attention tends to be in cyberspace.
- Their attention is not deployed in large blocks (in the way that previous generational cohorts at least claimed to do) but rather interleaved in smaller time

slices. They are often accused of multitasking everything; there is some truth to this but probably not as much as previous generational cohorts believe.

- They have been exposed to a much greater diversity of people and opinions. Their information sources are not just regional, not just national, but international by default. They can easily find text and video of people speaking other languages. They can encounter a wider range of opinions and contexts than any human could half a century ago.
- They have developed new ways of interacting, effectively a new etiquette for communication, so that the possibility of constant communication with a very large circle of acquaintances does not become intrusive. For example, because personal communication devices are always close, it is considered rude to send text messages at a time when the recipient is probably asleep. So contrary to stereotypes, Millennials have, and are, developing ways of managing an always-on world.

These characteristics of Millennials have implications for their behaviors in an organizational context, implications to which organizations will necessarily have to respond. Many of these implications are positive and provide a springboard for organizations to become more effective. Others are negative and require organizations to find new ways of dealing with them.

Some of the positive implications of the Millennial worldview are:

- They have discovered new ways of cooperating and creating that can be leveraged within organizations to build more holistic, dynamic and so responsive ways of working (Verdon 2012). As a concrete example, businesses whose products are digital, such as software or video, can use three shifts to get these products built more quickly—but these shifts take place in three different physical locations, each spaced eight time zones apart. Building products collaboratively this way requires detailed and regular interaction with members of other cultures, which Millennials are well-equipped to do (Myers and Sadaghiani 2010).
- They are members of a much wider number of interlocking communities than previous generational cohorts (Statistics Canada 2008). As a result, they provide organizations with a greater, and more diverse, reach. Their membership in these communities is longer-lasting, effectively, for example, discouraging organizations from short-term drive-by marketing and encouraging long-term permission-driven marketing. It also provides them with a competitive edge, for example in job hunting (Pew 2010: 9).
- They are sophisticated consumers of diverse sources of information. As a result, they are used to cross-referencing and triangulating information they are given, including that from within their organizations. Management strategies that involve holding back information will not be well received by Millennials, who expect to be told what is going on (Myers and Sadaghiani 2010).
- They believe that technology increases productivity and efficiency (Pempek et al. 2012).

- Despite the stereotypes of Millennials constantly checking their phones, they use time productively. In particular, they devote time to community activity in a way that previous generational cohorts do not. This is partly because the barriers to doing so have been lowered by technology; and partly because it can be done in smaller chunks (Shirky 2008). Computational tools remember context, reducing the effort of returning to a task in progress, and so enabling productive work to be done in smaller increments.

Organizations can, therefore, expect Millennials to be at least as productive as previous generational cohorts, but in novel ways that may require some adjustments. Their view of community is richer than that of previous generational cohorts, creating new opportunities for many kinds of organizations.

However, there are some negative implications of the Millennial worldview, and many of these are relevant to security. Some of these implications are:

- They prefer broadcast channels (many-to-many) rather than the one-to-one or one-to-many channels provided by email (Fritzon et al. 2007). In a fundamental way, communication is conceived as a multilogue, a conversation, rather than as a dialogue. They have been called "ambient broadcasters" (Pew 2010: 17). Furthermore, the audience component of a communication is often not a coherent shared-interest group but something more ad hoc ("friends") (Jacobs and Diefenbach 2012). This creates a plethora of problems:
  - There is a weaker match between content and receivers. A mailing list has some internal coherence that a group of friends or followers may not. Communications can be easily misconstrued, as a recipient does not necessarily have enough of the context to understand their full meaning.
  - Dissemination is not controllable by the original sender, and the technology makes it easy to pass communications on, far beyond their intended reach.
  - There are no gatekeepers to control what does and does not get disseminated—individuals decide for themselves (Johnson and Kaye 2010: 326).

  For organizations, this has the Comment: I do not see Beer 2014 anywhere. Beer 2009 is referenced potential for public relations and security disasters.
- Millennials, because they act in an interleaved fashion, do not have a strong sense of role, time, and place. Whereas previous generational cohorts might consider whether or not LOLcat emails were appropriate for organizational email, Millennials are less likely even to conceptualize that their work and leisure roles might require different decisions. In their lives, cyber and physical space blend in a way that is not the case for preceding generations (Harris 2014). From a security point of view, this means less sensitivity about whether, say, a potential organizational decision should be mentioned outside the organization.
- Similarly, they are likely to distinguish less between being "at work" or not, being used to dealing with work issues outside of normal working hours. The idea of not making personal calls during business hours is totally foreign to them. They are willing to deal with non-work issues during working hours.

In front-facing consumer-service businesses this already creates management issues. For the same reasons, they have less sense of being physically at work, and so might perhaps work on confidential organizational business at a local coffee shop, unaware of any security concerns. (Of course, this also means that they are likely to "work" even during leisure time, which can be to an organization's advantage.)

- Their sense of privacy is different to that of most adults from the second half of the 20th Century (Pew 2010: 8). At the mundane level, they are accustomed to living their lives under the pervasive gaze of cultures of social surveillance (Bauman et al. 2014: 141–142) as exemplified by social media sites that disseminate their personal information widely within the social media framework, and also leverage it by selling it to other organizations. It is not yet clear whether Millennials do not *realize* that their personal information is not only widely spread but also archived for the foreseeable future, or whether they do not *care*, feeling that living life in the open is natural and appropriate (Accenture 2008; Fritzon et al. 2007). Millennials thus find the imposition of privacy and security irksome at best, and something to resist at worst.
- Because of their use of personal devices and software that knows their location, organizations must take into account that their employees' locations are essentially public information. This is of particular concern, of course, for organizations such as police and armed forces (Hibbard 2011; Drapeau and Wells 2009).
- Millennials will provide their own technology when employers are unable or unwilling to oblige (Accenture 2008). Where previous generational cohorts expected their employers to provide the necessary tools for work, Millennials are predisposed to short-circuit this process. For example, organizations that provide employees with smart phones to ensure their availability may replace these devices on a two-year cycle; much longer than the 6-month or shorter cycles that smart phone makers use. As a result, Millennials may just buy leading-edge smart phones in place of those provided. There are security implications when these (unauthorized and perhaps unrealized) devices are used for organizational activities.
- Similarly, if the software tools provided by an organization are deemed inadequate by Millennials, they are perfectly comfortable acquiring others, perhaps open-source freeware and even installing them on the organization's systems. Again there are security implications.

Millennials and their attitudes, many of which are present in older cohorts albeit at lower intensities, represent challenges for organizations. Many of their characteristics are positive and represent considerable potential for new organizational paradigms. However, from a security perspective, these characteristics create potential vulnerabilities that organizations have perhaps not yet fully realized, and for which good responses are still unclear.

5 Conclusion: Data Assurance in Compromised Environments

The Castle Model for organizational, and especially network, security is based on layers of walls that define, very strictly, what is inside and what is outside. This model, at least in the cyber domain, has never been very effective. We have suggested that three forces are eating away at this model as a practical security solution. First, organizations themselves tear down their walls and make their gateways more porous because it pays off in terms of better agility and responsiveness—they can do more, faster and better. Second, technological developments increasingly destroy walls from the outside as computation becomes cheaper, and as the implementation of virtual walls and gateways becomes more complex, and, therefore, contains more vulnerabilities to be exploited by the clever and unscrupulous. Third, changes in the way humans and technology interact, exemplified by the Millennial generation, blur and dissolve the concepts of inside and outside, so that the distinction becomes invisible, or even unwanted, and boundaries become either anachronisms or annoyances to be circumvented.

Moreover, the Castle Approach to cybersecurity is marred by a fundamental ethical problem: access to the model is a function of finances, as the degree of protection afforded correlates loosely with sunk costs invested. The rise of the cybersecurity industry is evidence to that effect (Zedner 2009; Gill 2006). The Castle Model thus directly reinforces the digital divide, and indirectly the digital divide's economic and social fault lines among individuals, households, businesses, geographic areas, class, race, ethnicity, and gender across the globe (Castells 2001; Norris 2001; Lu 2001; National Telecommunications and Information Administration 1995). Ethically, any model of cybersecurity that reinforces privilege and, arguably, power relations, is necessarily problematic: as with physical security, cybersecurity should not be parceled out by financial means.

What can be done in a world where the separation between inside and outside is so porous as to prevent hardly anything? Organizations still need to get work done without it being visible to the rest of the world, including their competitors and others whose interests are in opposition. It seems clear that the solution is not to "fix" the three forces that have driven us to the current situation. Organizations may not have consciously decided to weaken boundaries to achieve greater agility, but it has been successful nevertheless. While technology may provide some limited improvements in virtual wall techniques, it is clear that, as ever, the advantage is with attackers. And it is hopeless to imagine that Millennials, and their successor cohorts can be convinced to cut themselves off from the networked world just because they are "at work".

A new kind of solution is needed (Karas et al. 2008). Although still in its infancy, the most hopeful direction to protect data is a strategy known as *computing in compromised environments*. Its goal is to allow organizations (and individuals) to do useful and confidential things in cyberspace, even in the face of the issues we have been discussing. Techniques for computing in compromised environments must allow useful work to be done even if an attacker is already inside the castle. There may still be a role for walls, but only as impediments, and not as protection.

Ways to do this are the subject of active research, so it is only possible to give some flavor of the ideas under consideration, which include:

- Operating in virtual castles. Virtual machines run on top of physical computers and can emulate the software that would normally run directly on top of the hardware. However, a virtual machine can be created as needed, and destroyed when its usefulness is over. Furthermore, each virtual machine can be configured randomly to be slightly different. This makes it difficult for an attacker to target the task the virtual machine is carrying out because a generic attack can no longer be used—they must first work out which variant is actually in use, and then develop and launch a customized attack. The time window in which this sequence must be carried out has to be smaller than the existence time of the virtual machine.
- Operating with virtual software. Much popular software has known vulnerabilities that are compensated for by malware detectors and regular software updates. However, so-called zero day exploits—vulnerabilities that are not known to the software creators—remain a problem. It is now possible to create a piece of software to carry out some task using pieces of code found in other places in the system (a kind of software Frankenstein's monster). The advantage of such created-on-the-fly software is that it will be different each time; so, knowing a vulnerability in the official, static version of the software does not mean that any particular occurrence of the actual software will contain it.
- Modelling at the level of behavior or intent rather than at the level of moving bits. Wall technologies tend to focus on what is crossing the boundary and passing through the gates. Once an attacker in "inside" there is often much less scrutiny. Behavior modelling tries to understand the *intent* of traffic and actions, so that activities whose individual pieces look innocuous can be detected at a more abstract level. This is the sort of traffic monitoring to which signals intelligence agencies are heavily committed.
- Using secret sharing. Secret sharing allows two or more people to hold individual pieces of information that, on their own, are useless but that, when assembled, reveal some secret to one or more of them. As with safeguards against accidental nuclear launches, systems can be created so that any number of participants must share their piece for the entire secret to be revealed.

  Secret sharing can provide an alternative to passwords. As a simple (and artificial) example, a system may provide a user who wants to authenticate with a latitude. The user's correct response is a country with an A in its name that lies on that latitude line. If the system generates the latitude value randomly, it takes a very large number of observations of the challenge-response pair even to begin to guess the rule—but all the user needs is a globe.
- Use multiple versions of all files and use secret sharing to allow users to work with the true ones. Suppose there is a document that the organization does not want exfiltrated. The system creates multiple copies of this document, one the

true one, and the others false. The false ones need not look artificial—the Frankenstein mechanism already discussed means that they can be created from pieces of true documents so that there is no easily automated way to tell, from the content, the true from the false.

Of course, users want to edit and read the true documents and ignore the false ones. Secret sharing can be used to identify which one is the true one. Suppose, for the sake of a simple example, that there is one true version and one false version. The system generates a fixed-length bit string *Y*. Offline the user is given the bit string that results from computing the exclusive-or of a secret bit string, *S*, and *Y*. When the user wants to access a file, the system provides *Y*, the user (offline) computes the exclusive—or of *Y* with the given string (*S xor Y*) which recreates *S*. If the parity (the number of one bits) in S is even, the true document is document 1, otherwise the true document is document 2. Knowing *Y* doesn't help someone else, even an insider, to know which version to exfiltrate; even if the user writes down (*S xor Y*) and leaves it visible, this isn't enough to identify the version to exfiltrate.

This simple idea can be generalized to much larger scale and there are many ways to encode the partial secrets. Furthermore, the true version can be swapped around, can appear to be differently named for different users, and the secrets can be altered easily and cheaply.

These ideas are still in the early stages of development. However, they seem to hold more promise than attempting to continue to build higher and thicker walls, and persuade users not to dig through them, open the gateways from the inside, or circumvent them in other ways. The history of real castles is an object lesson of the weakness of the more-and-better-walls strategy; and of the failure to grasp the sociology of cyber security being posited in this article, and its operational, conceptual and theoretical implications.

References

Accenture (2008) Millennials at the Gates: results from Accenture's High Performance IT Research. Accenture Research USA, New York

Agamben G (1999) Potentialities. Stanford University Press, Stanford

Bauman Z, Lyon D (2013) Liquid surveillance: a conversation. Polity Press, Cambridge

Bauman Z, Bigo D, Esteves P, Guild E, Jabri V, Lyon D, Walker RBJ (2014) After snowden: rethinking the impact of surveillance. Int Polit Sociol 8(2):121–144

Beer D (2009) Power through the algorithm? Participatory web cultures and the technological unconscious. New Media Soc 11(6):985–1002

Bloomberg Business (2011) Human errors fuel hacking as test shows nothing stops idiocy. http://www.bloomberg.com/news/articles/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy. Accessed 30 June 2011

Castells M (2001) The internet galaxy: reflections on the internet, business, and society. Oxford University Press, Oxford

Common Vulnerabilities and Exposures, MITRE (2013) Heartbleed. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160. Accessed 1 April 2013

Deloitte (2012) Tech Trends 2012: elevate IT for digital business; a federal perspective. Deloitte LLP Services, London. http://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-cons-tech-trends-2012.pdf. Accessed 1 April 2015

Drapeau M, Wells L II (2009) Social software and national security: and initial net assessment. Center for Technology and National Security Policy. National Defense University, Washington, DC

Fritzson A., Howell LW, Zakheim DS (2007) Military of Millennials. Strategy + Business 49. http://www.strategy-business.com/article/07401?pg=0

Foucault M (1991) Discipline and punish: the birth of a prison. Penguin, London

Foucault M (1998) The history of sexuality: the will to knowledge. Penguin, London

Frincke DA, Bishop M (2004) Guarding the castle keep: teaching with the fortress metaphor. IEEE Secur Priv 2(3):69–72

Gill M (2006) The handbook of security. Palgrave Macmillan, New York

Goldsmith A, Brewer R (2015) Digital drift and the criminal interaction order. Theoretical criminology. Forthcoming

Harris Michael (2014) The end of absence: reclaiming what we've lost in a world of constant connection. Current, Toronto

Harknett RJ, Stever JA (2011) The new policy world of cybersecurity. Public Adm Rev 71 (3):455–460

Hershatter A, Epstein M (2010) Millenials and the world of work: an organization and management perspective. J Bus Psychol 25(2):211–223

Hibbard L (2011) Communicating with the net generation. U.S. Army War College, Carlisle Barracks, PA

Jacobs J, Diefenbach V (2012) The use of social media in public affairs—a German perspective. North Atlantic Treaty Organization RTO-MP-HFM-201, Brussels

Johnson TJ, Kaye BK (2010) Believing the blogs of war? How blog users compare on credibility and characteristics in 2003 and 2007. Media War Confl 3(3):315–333

Karas TH, Moore JH, Parrott LK (2008) Metaphors for cyber security. SANDIA report SAND2008-5381. Sandia National Laboratories, Albuquerque

Lee CKC, Conroy DM (2003) Teenager's consumption on the internet. Australas Mark J 13(1):8–19

Leydesdorff L (2010) The communication of meaning and the structuration of exceptions: Giddens' 'structuration theory' and Luhmann's 'self-organization'. J Am Soc Inform Sci Technol 61(10):2138–2150

Lu M (2001) Digital divide in developing countries. J Global Inf Technol Manage 4(3):1–4

McDougal M (2009) Castle warrior: redefining 21st century Network defence. In: CSIIRW '09 proceedings of the 5th annual workshop on cyber security and information intelligence research: cyber security and information intelligence challenges and strategies. http://www.cisr.ornl.gov/csiirw/09/CSIIRW09-Proceedings/Abstracts/McDougal-abstract.pdf. Accessed 25 May 2015

Myers KK, Sadaghiani K (2010) Millennials in the workplace: a communication perspective on millennials' organizational relationships and performance. J Bus Psychol 25(2):225–238

National Telecommunications and Information Administration (1995) Falling through the net: a survey of the have nots in rural and urban America. U.S. Department of Commerce, Washington, DC

Norris P (2001) Digital divide: civic engagement, information poverty, and the internet worldwide. Cambridge University Press, Cambridge

Pariser E (2012) The filter bubble: how the new personalized web is changing what we read and how we think. Penguin Books, New York

Pew Research Center (2010) The future of the internet. http://pewinternet.org

Quigley K, Roy J (2012) Cyber-security and risk management in an interoperable world: an examination of governmental action in North America. Soc Sci Comput Rev 30(1):83–94

Resnyansky L, Falzon L, Agostino K (2012) From transaction to meaning: internet-mediated communication as an object of modeling. In: 8th International Conference on Social Science

Methodology. Sydney, 9–13 July, Conference Proceedings Vol II. http://itupl-ura1.ml.unisa.edu.au/R/?func=dbin-jump-full&object_id=116267. Accessed 3 May 2015

Sassen S (2002) Towards a sociology of information technology. Curr Sociol 50(3):365–388

Shirky C (2008) Here comes everybody: the power of organizing without organizations. Penguin Press, New York

Statistics Canada (2008) Canada′s Ethnocultural Mosaic, 2006 Census. Ottawa. http://www12.statcan.ca/census-recensement/2006/as-sa/97-562/pdf/97-562-XIE2006001.pdf

Tufekci Z (2008) Can you see me now? Audience and disclosure regulation in online social network sites. Bull Sci Technol Soc 28(1):20–36

Verdon J (2012) The wealth of people: how social media re-frames the future of knowledge and work. North Atlantic Treaty Organization RTO-MP-HFM-201, Brussels (April)

Zedner L (2009) Security. Routledge, Abingdon, chapter 5

Food Security as Critical Infrastructure: The Importance of Safeguarding the Food Supply for Civil Security

Anna Brinkmann and Karolin Bauer

Abstract Vulnerabilities in critical infrastructures can cause significant hardships to the affected population during crises and large scale disasters like Hurricane Sandy in 2012 or the nuclear catastrophic event Fukushima in 2011. Referring to this, critical infrastructures include "primary physical structures, technical facilities and systems whose disruption, failure or destruction have a serious impact on the functioning of society, the economy or the state within a natural hazard induced disaster context" (UNISDR 2011: 6). As a component of critical infrastructures, Food and especially the Food Supply is a significant part of the services for the public and fundamental for an effective Civil Security System. In this chapter primary definitions regarding Food as a critical infrastructure are depicted as the meaning of safeguarding the food supply in case of crisis or disaster situations emerges as critically important. Furthermore selected hazards and their impacts to the society are described.

Keywords Mitigating food supply risks · Food supply chain · Security · Critical infrastructure · Hazards · Lessons learned

1 Introduction

The vulnerability of critical infrastructures and its impact on the social and economic well-being are made clear by the multitude of risks by natural disasters (Masys 2014: 265). As constituent of the critical infrastructures, Food and particularly the Food Supply have a particular importance on the population's well-being and on securing the Civil Security (Ridley 2011: 7). Food as critical infrastructure is recognized for its critical importance to crisis and disaster management plans as well as the relevance of mitigating supply chain risks and promoting supply chain

A. Brinkmann (✉)
Fachhochschule Münster, University of Applied Sciences, Münster, Germany
e-mail: anna.brinkmann@fh-muenster.de

K. Bauer
Freie Universitaet Berlin, Münster, Germany

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_13

resilience. An exemplary concept of ensuring food supply in disasters is described as a case study and discussed later.

Considering this chapters' topic, **critical infrastructures** are seen as "organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences" (Federal Office for Information Security and Federal Office of Civil Protection and Disaster Assistance 2013). Masys (2014: 9) summarizes the importance of critical infrastructures as "the backbone of our nation's economy, security and health". Both definitions affirm the importance of critical infrastructures: on the one hand they confirm the significance of ensuring critical infrastructures to the Civil Security and on the other hand they signify its importance on (Food) Supply as critical infrastructure. According to the Federal Office for Information Security and Federal Office of Civil Protection and Disaster Assistance in Germany (2013), critical infrastructures could be subdivided into the following sectors: State and Administration; Energy; Health; Information, Technology and Telecommunication; Transport and Traffic; Media and Culture; Water; Finance and Insurance; Food (Federal Office for Information Security and Federal Office of Civil Protection and Disaster Assistance 2013; cf. Fig. 1). The division of the mentioned

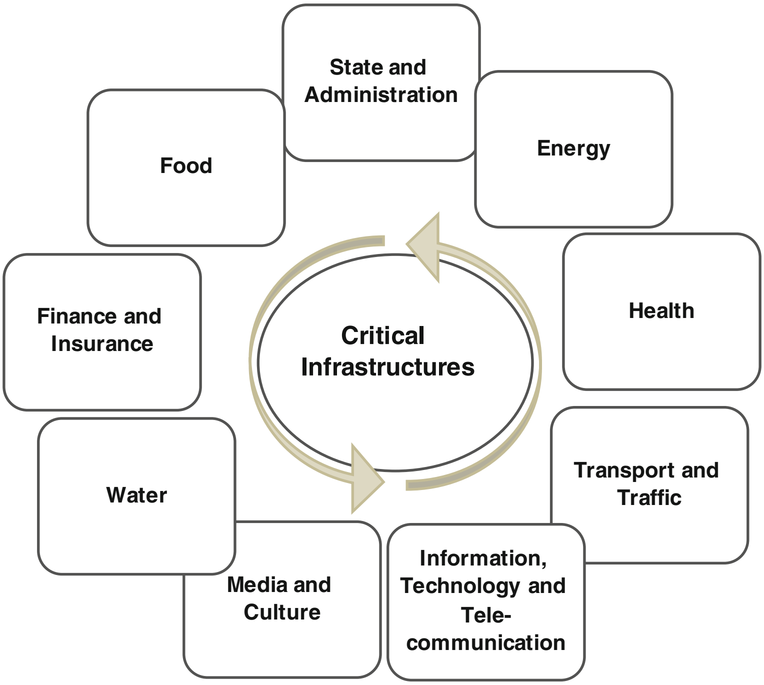


Fig. 1 Critical infrastructures. *Source* According to Federal Office for Information Security and Federal Office of Civil Protection and Disaster Assistance (2013)

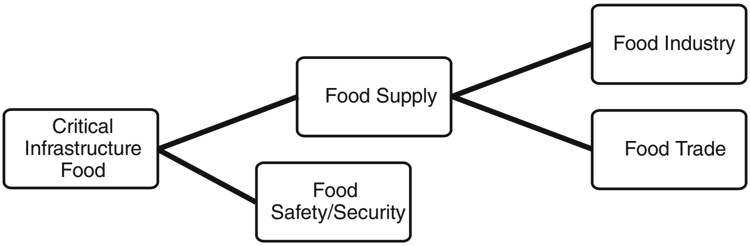


Fig. 2 Subdivisions of the critical infrastructure food. *Source* Ridley (2011: 7, 14), OECD (2008: 3), Government of Netherlands (2015)

sectors and the definition of the term "critical infrastructure" are in most of the industrialized countries applied and similarly defined. In general the term critical referring to infrastructures describes infrastructure whose disruption would induce far-reaching and disastrous damage (OECD 2008: 5).

As pictured in Fig. 1, each sector among the critical infrastructures includes particular arrangements, but the critical infrastructures among one another are "characterized as complex coupled networks with inherent interdependencies and interconnectivity. […] Because of these interdependencies within and across critical infrastructures, failures within one network may cascade through dependent nodes in other networks" (Masys 2014: 266). Therefore in case of any disruption of one of the critical infrastructures, most of the others are affected, too. Hence the most risky vulnerability of critical infrastructures is hidden in the interdependencies across and among the many different infrastructures (Masys 2014: 272) (Fig. 2).

Ridley (2011) describes the relation among the infrastructures as follows: "The interface where interaction takes place among the corporations supplying the infrastructure goods or services, users and other stakeholders, is often complex. For example, although community safety requires access to health services and provision of electricity, multiple parties are involved in these two exchanges" (Ridley 2011: 7). In addition, the government is involved in these dependencies. In summary, safeguarding critical infrastructures "underpins economic growth and promotes social well-being, certainty and confidence" (Ridley 2011: 7).

As described, critical infrastructures are complex coupled networks. Considering this, the disruption of one critical infrastructure sector often causes broader, so-called **cascading-effects**. The magnitude of the impact of an incident can increase significantly by cascading effects (Zimmermann and Restrepo 2009: 1). The cascading-effect entitles a contingent process provoked by a disruption or failure within the critical infrastructures, which potentially can cause failures in further sectors of critical infrastructures and have negative effects on society. In addition the national economy as well as the citizens' confidence in the political leadership can be seriously impaired by "immediate damage caused to affected persons" (Federal Republic of Germany 2009: 9). Ridley (2011) has given the following example referring to the negative consequences of cascading-effects: "The fragility of critical infrastructure and the capacity of the problem to cascade to other sectors and industries were demonstrated by the 2003 power blackouts. The blackouts started with an electricity supply problem in Idaho but impacted 50 million people in the North East of the United States (US) and Ontario, Canada. The outage led to loss of function of airports, banks, mobile phones, passenger trains, computer systems and the New York Stock Exchange" (Ridley 2011: 7f). Considering this, the challenge is to comprehend in which way these interdependencies operate and how to mitigate the cascading-effects (Zimmermann and Restrepo 2009: 1). Therefore it would be useful to conduct analysis referring the resilience of the infrastructures against unplanned incidents as well as against unknown cascading-effects (Masys 2014: 276).

Civil Security (also: civil protection, national security and public security) aims at the protection of all civilians of a nation against various kinds of threats (direct and indirect) (Kirchner et al. 2012: 3). Civil security systems include "policies, bodies and mechanisms that a country or region has in place to protect it against new and urgent threats to the security of people and/or the functioning of critical infrastructures" (Swedish Institute of International Affairs 2014: 5). Thus, there is a direct correlation between critical infrastructures on the one hand and civil security on the other hand.

The next section focuses on the meaning of food as critical infrastructure and the importance of ensuring the food supply in crisis or disaster situations.

2 Safeguarding the Critical Infrastructure: Food Security

2.1 Food as Critical Infrastructure

Food, as a CI, is used in the meaning of food supply including the subsectors food industry and food trade (including in supermarkets) as well as the food safety/security (Federal Office for Information Security and Federal Office of Civil Protection and Disaster Assistance 2013; OECD 2008: 3; Government of Netherlands 2015).

With regard to Civil Security and securing critical infrastructures **ensuring food supply** means: "The capacity to maintain the basic activities that are indispensable for safeguarding the populations living conditions, for sustaining the functioning of critical infrastructures, and the material preconditions for maintaining national preparedness and defense in case of emergency conditions and serious disturbances" (Ministry of Defence 2011: 95).

According to the Security, Federal Office for Information and the Federal Office of Civil Protection and Disaster Assistance in Germany (2015), **Food Supply** as critical infrastructure "is undertaken mainly by the private sector. The public sector still assumes the central role in the assurance of food quality as the supervisory authority and in regulating food supply in crisis situations. The protection of the Critical Infrastructure Food includes the maintenance of the food supply itself, as well as the supply in crisis situations and the maintenance of basic services, which are relevant to the food supply, such as the electricity supply, water supply and transportation" (Federal Office for Information Security and Federal Office of Civil Protection and Disaster Assistance 2013). For instance, the transportation and in particular the railway industry in Britain has a "significant impact on the British way of life, assisting citizens in many ways. It facilitated the mass production of many products including food, beer, building supplies and manufactured goods, and enabled them to be transported to almost any location in Britain, lowering prices and widening choice" (Ridley 2011: 14).

By analyzing the understanding of critical infrastructures in an international context, it could be assumed that the Food sector is an explicit part of the complex network of critical infrastructures in most of the industrialized countries. Also according to OECD (2008: 4f, 7), Food is a component of most of the countries sectoral coverage of Critical Infrastructure Plans. It is revealed that the critical infrastructure Food (and also water) is an officially determined constituent of the critical infrastructures network of Australia, Canada, the Netherlands, the United Kingdom, and the United States as well as in the European Union. For a better understanding of dependencies and capacities with regard to the critical infrastructure Food (Supply) it seems to be important to describe the basic information of Food Supply and in particular referring to Supply Chains.

Figure 3 illustrates the complexity and the **dependencies** within the food supply process. There are plenty of impacts (from other critical infrastructure sectors) influencing the steps from food production over Food processing and packaging, food distribution, Grocery Retail and Food Services to the Consumers. For example, if goods for the food production can't be delivered because of a failure in

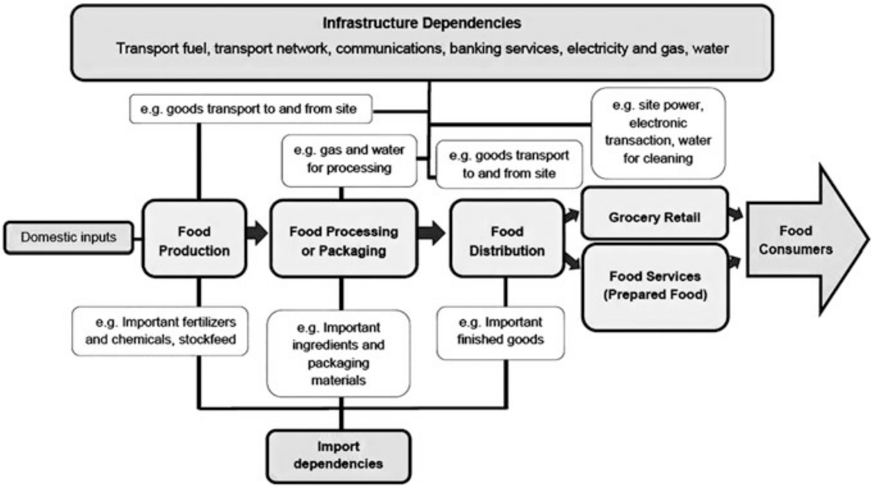

Infrastructure Dependencies
Transport fuel, transport network, communications, banking services, electricity and gas, water
e.g. goods transport to and from site
e.g. gas and water for processing
e.g. goods transport to and from site
e.g. site power, electronic transaction, water for cleaning
Domestic inputs
Food Production
Food Processing or Packaging
Food Distribution
Grocery Retail
Food Services (Prepared Food)
Food Consumers
e.g. Important fertilizers and chemicals, stockfeed
e.g. Important ingredients and packaging materials
e.g. Important finished goods
Import dependencies

Fig. 3 Overview of the food supply and its dependencies. *Source* Acc. Commonwealth of Australia (2011: vii)

the traffic infrastructure as a result of a blizzard, the following process steps will be constricted or they couldn't be realized (Fig. 3).

Considering Fig. 3 and according to the report "Resilience in the Australian Food Supply Chain" of the Commonwealth of Australia (2011), a few key vulnerabilities referring to maintenance of food supply (resilience) emerge (Commonwealth of Australia 2011: ix):

- concurrent loss of a number of distribution center facilities,
- concurrent loss of a number of transport links to and between major cities,
- shortage of fuel (diesel) for food distribution in the case of a national fuel emergency,
- ongoing workforce availability constraints beyond which affected companies can manage using standard backfilling and casual pool arrangements,
- extended material disruption (of materials strongly dependent on imports).

In order to mitigate the potential impact during major disasters, it seems to be absolutely necessary to investigate what are potential threats to the critical infrastructure and how the food supply can be ensured.

2.1.1 Safeguarding the Food Supply Chain

The food sector is characterized by ownerships in the private sector. Because of increasing dynamic complexity within the global food networks and the business environment, it is becoming more important to the stakeholders to analyze and identify supply chain risks (Dun and Bradstreet 2011: 9).

2.1.2 Mitigation Supply Chains Risk

Similar to approaches for crisis management in general, there are also some approaches to mitigate Supply Chain Risks or rather "to build a culture of awareness over threats" (Dun and Bradstreet 2011: 9) to safeguard supply chains. For example, the Trusted Information Sharing Network for Critical Infrastructure Protection of Australia (2012: 1) elaborated a strategy to address the key gaps and vulnerabilities. In this regard, arrangements to increase the preparedness and to facilitate developing and conducting plans to secure the Food sector are subdivided in the following five themes identified: Communication, Prevention, Preparedness, Response and Recovery.

There are some important fundamentals and approaches to mitigate supply chain risks according to Harris (2015):

- Food, grocery and other products use sophisticated supply chain and logistics management systems;
- "Just in time" management reduces redundancy in the food supply chain;
- Food sector business continuity means provision of essential products as usual under most circumstances;

- Government relief and recovery can harness resources and expertise from the sector;
- Joint planning is required;
- Risks + Learning + Collaboration = Opportunities.

2.1.3 Promote Supply Chain Resilience

Resilient critical infrastructures are an essential requirement for national security. In general, **resilience** refers to the "capacity of organizations or systems to return to full functionality in the face of disruption" (Commonwealth of Australia 2011: viii). Barack Obama (President of the USA) for example instituted the Presidential Proclamation Critical Infrastructure Security and Resilience (2014). This proclamation suggests the importance of securing the Nation's resources, reduce vulnerabilities and enhance the critical infrastructures resilience by for instance information, cooperation and training (The White House. Office of the Press Secretary 2014). Enhancing the infrastructures resilience, as depicted in the National Infrastructure Protection Plan, "depends on the ability of public and private critical infrastructure owners and operators" (Homeland Security 2013: 1). Considering this, within the Presidential Proclamation an approach to promote resilience is described. This includes the integration and cooperation of different stakeholders e.g. by informing and educating them in an active and direct way (The White House. Office of the Press Secretary 2014).

The following (management) systems and models to promote and improve the resilience of Food Supply relating to crisis and disaster situations are listed (Commonwealth of Australia 2011: 25f; Harris 2015):

- Communication and network development
- Security risk management
- Business continuity
- Inter dependencies (e.g. between power, gas, water, transport)
- Emergency preparedness and links with the emergency services
- Surge capacity
- Preparedness to assist manage the food supply after a catastrophe.

The emerging challenges with regard to ensuring the food supply in crisis and disaster situations are described by means of questions below-structured into the scale factors, scope factors, temporal factors, distributional factors and industry factors. (Commonwealth of Australia 2011: ix) Table 1.

Again, it becomes apparent that these mentioned factors are mostly referring to the food supply chain, which can be seen as basic elements of the Food sector with regards to the society and the populations' provision during and after crisis or disaster situations.

More practically and with regards to the food sector/industry, there should be provision for an adequate availability of (food) stocks and inventory within the

Table 1 Factors on ensuring food supply

Scale factors
Can the food supply chain *adapt to disruption up to a certain population or geographic scale, with elements breaking down beyond that point*?
Scope factors
Can the food supply chain *adapt to disruption for particular types of foods or inputs to foods up to a certain level of scope, with elements breaking down beyond that point*?
Temporal factors
Can the food supply chain *manage a resilient response to a disruption for a certain period of time, with elements breaking down beyond that point*?
Distributional factors
Is the food supply chain *less resilient for some sections of the community than others (such as low income households, tourists)*?
Industry factors
Are *some sections of the industry, by function or product type,* […] *less resilient than others given their particular circumstances, and any dependencies across industries*?

Source Acc. to Commonwealth of Australia (2011: ix)

supply chain and an appropriate "availability of manufacturing capacity" (including product manufacture as well as bottling and canning capacity). The transport capacities (e.g. railway rolling stock, trucks and shipping) as well as the transport route should be known, secured and if necessary there should be a number of alternative transport ways available in order to ensure the raw material- and product-transportation. Furthermore it is important to safeguard handling and storage facilities like loading, forklift trucks and packaging (Commonwealth of Australia 2011: 19).

But it also should be remarked that on the one hand prevention and preparedness plans are useful and can avert plenty of hazard effects. But on the other hand "it is neither possible nor economically sensible to attempt to deal with every risk" (Trusted Information Sharing Network for Critical Infrastructure Protection 2012: 1).

2.2 Case Study: Emergency Food Services (Canada)

The third largest province in Canada, British Columbia, exemplifies an efficient possibility for ensuring food supply in times of crisis. The concept named Emergency Food Service is part of the Emergency Social Services of the Provincial Emergency Program. In general this Emergency Social Services include the category groups Emergency Clothing Service, Emergency Lodging Service, Emergency Food Service, Registration and Inquiry Service as well as Personal Services and Reception Centre Service (Government of British Columbia 2006; Authority of the

Minister of Health 2007: 11f). It aims at providing disaster victims with the mentioned essential services. Government agencies and community organizations are responsible for developing and conducting the basic Emergency Social Services plans (Authority of the Minister of Health 2007: 11f). Potential participants may include (Authority of the Minister of Health 2007:12):

- *Municipal or provincial departments of social services, public health, mental health, family and children's services,* etc;
- *Private social service agencies;*
- *Service clubs, church groups, branches of national organizations;*
- *Business and professional associations.*

In particular, the Emergency Food Service should meet the urgent needs of and provide food for people who cannot feed themselves or who are without food provisions or/and food preparation facilities. Furthermore it aims at provisioning and recovery of workers and volunteers. Special attention is centered on requirements of risk-groups comprising infants, children, pregnant women, nurses, the elderly, sick persons (e.g. diabetics) and disaster workers (Authority of the Minister of Health 2007: 13). Essential considerations, which are listed in the referring concept "Emergency Food Service: Planning for Disasters" contain for instance food requirements as well as available supplies, staff and facilities. In addition, religious and cultural particularities referring to the affected population and aspects of the Public Health should be considered (Authority of the Minister of Health 2007: 13).

In summary, the Canadian Emergency Food Service seems to be an integrative, cooperative and multi-stakeholder concept, which benefits from the different stakeholders excellence to ensure the populations provisioning.

3 Hazards and Their Impacts on the Critical Infrastructure Food

It seems to be important to specify types of hazards and their impacts on the critical infrastructures of the food supply. Therefore two examples of past disasters are given to illustrate different impacts on the food supply. Furthermore, ways to reduce the impact on the food supply regarding the population are shown. Lastly, various lessons learned examples of the two presented past disasters are pointed out.

3.1 Exposure to Hazards and Past Disasters Regarding the Food Supply

"Natural hazards afflict all corners of the earth, often unexpected seemingly unavoidable and frequently catastrophic in their impact" (Bryant 2005: i). Over the past decades, the intensity and frequency of natural disasters is increasing. Findings of Muenchener Rueckversicherungs-Gesellschaft illustrate that the number of natural disasters doubled since 1960 (Rueckversicherungs-Gesellschaft 2015: 16). Damages resulting from natural hazards have quintupled causing loss of human life, damage to goods and infrastructures at the local, regional and global scale (Ruckversicherungs-Gesellschaft 2015: 16). The term natural hazard which is used by the authors follows the definition of the UNISDR: "Natural processes or phenomena occurring in the biosphere that may constitute a damaging event. [...] Hazardous events can vary in magnitude or intensity, frequency, duration, area of extent, speed of onset, spatial dispersion and temporal spacing" (UNISDR 2009: 20f).

The definition of the term "natural hazard" shows the complexity of the problem space highlighting that the estimation of temporal spacing of an occurring natural hazard is barely or not possible. Furthermore there are difficulties in estimating the intensity and area of extent. Besides natural hazards there are man-made (e.g. September 11 attacks), technical, nuclear hazards (e.g. Fukushima 2011) etc. which can have disastrous impacts if they occur. A hazard is a threat, not the actual event. Any hazard can lead to an actual harmful event (Thywissen 2006: 36). Therefore disasters are a result of the exposure to a hazard. The impacts of disasters are "serious disruption(s) of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources." (UNISDR 2009: 9).

If a disaster occurs there are elements at risks which are affected by the impact resulting from hazards (Thywissen 2006: 36). Elements most at risk are population, buildings, infrastructures, components of the environment (e.g. landscapes) and economic components (e.g. business activities) (Federal Office for Information Security and Federal Office of Civil Protection and Disaster Assistance 2013). Because of the increasing complexity of different social, economic and cultural aspects, natural hazards tend to lead to cascading effects of CI and increase their impacts and damages in urban landscapes (Kuhlicke et al. 2012: 29). The information about the critical infrastructure of the food supply is quite important for prevention, planning and preparedness in context of minimizing the impacts at regional, national or international scale.

3.1.1 Ensuring the Food Supply During Past Disasters

As mentioned above, Critical infrastructures are complex and interdependent systems which are vulnerable to threats from natural and man-made hazards (Table 2). To picture which impacts on the food supply can occur during disaster events two examples are given: The Queensland Floods (Australia) and Hurricane Sandy (USA).

Table 2 Examples of major events that may test food supply chain resilience

Event type	Example
Pandemic	Possible influenza pandemic
Electricity or gas supply outage	2009 Victorian Black Saturday bushfires
	2008 Western Australian gas crisis—Veranus Island
	1998 Victorian gas crisis—Longford explosion
Industrial action	2008 national road transportation driver shutdown
	1998 waterfront strike
	1987 storemen and packers strike
Food or water contamination	1998 Sydney water contamination incident
Severe weather event (flood, cyclone, drought)	2011 tropical cyclone Yasi
	2010/11 Queensland floods
	2010 tropical cyclone Ului—Queensland (Airlie Beach)
	2010 central Queensland flooding
	2007 Sydney supercell storm
	2007 Hunter Valley floods
	2006 tropical cyclone Larry—Queensland
Other possible events	Coordinated demonstrations
	Land contamination (chemical) in production areas
	Major animal or plant disease biosecurity emergency

Source Commonwealth of Australia (2011: 21)

Queensland Floods (Australia)

The Australian Government (Department of Agriculture, Fishery and Forestry) provides examples of major events that may test the food supply. One of the main disasters affecting the food supply during the past were the Queensland floods in 2010/11. An extensive rainfall caused flooding over extensive areas of Queensland in December 2010 into January 2011 (Queensland Floods Commission of Inquiry 2012: 32). The floods caused the death of 33 people: three people remain missing. Almost 80 % of the Queensland state was declared a disaster zone. About 2.5 million people were affected and almost 30,000 homes and businesses were inundated (Queensland Floods Commission of Inquiry 2012: 32). Cutting of transport routes caused by the flood led to temporary shortages of food items. Subsequently, manufacturing of food products like bread, milk and meat was disrupted (Commonwealth of Australia 2011: 25). With regard to population's behavior both in affected and unaffected areas, panic buying was observed. "A factor determining whether a community was prone to panic buying was consumers' familiarity with disasters: some commented that newer Queensland residents were more prone to panic buying than longer-term residents" (Commonwealth of Australia 2011: 31). Due to implemented business continuity planning, food service industry limited the impact of panic buying although they experienced disruption of the food supplies (Commonwealth of Australia 2011: 31). Another factor of impact illustrates the inundation of food facilities. "For these (cases), restocking became the immediate priority" (Queensland Floods Commission of Inquiry 2012: 32).

Hurricane Sandy (USA)

In October 2012, Hurricane Sandy with heavy rains, strong winds and significant storm surges hit the Caribbean and eastern United States. The Hurricane killed 69 people in the Caribbean and took 73 more lives in the US. Hundreds of thousands of homes were damaged and residents were forced into shelters. Main parts of the infrastructure systems like power and water supply as well as the transport system were affected. The food and water supply was impaired particularly in New York, New Jersey and Connecticut. Food shortages were observed. 'State and local governments took a leading role to prepare their communities for the disaster and mobilize once the storm hit' (Bucci et al. 2013: 2). Relief Organizations like the Salvation Army mobilized feeding units to serve thousands of meals in the affected areas. The United States has wide range of experience dealing with emergency situations (e.g. hurricane and tornado seasons), which are mostly limited on the regional or local level. Therefore local or regional emergencies allow a compensation of the food supply through food supply transportations from unaffected parts of the US. In the case of Hurricane Sandy and the affected greater area of New York and damaged and impassable bridges and tunnels, lead to challenges associated with keeping up the food supply. Outages of the power supply hindered cleanup and transportations to so called entry points for supplies.

3.1.2 Lessons Learned from Past Disasters

Lessons Learned from past hazardous events and disasters can be used to develop scenarios, new methods and open up new research. Learning from the past and implementing knowledge and experiences can increase the ability to understand future impacts on the food supply.

The Federal Agency of Emergency Management (FEMA) describes Lessons Learned as "Lessons learned are knowledge and experience (both positive and negative) derived from observations and historical study of actual operations, training, and exercises." (Blanchard 2008: 683). Therefore, the main aspects of Lessons learned depends on experiences as a sum of valid and well-grounded knowledge, whether they are positive or negative findings (Deutsches Komitee Katastrophenvorsorge eV 2004: 8). In this context, there is a demand to enhance information sharing across international stakeholders of the food supply. Information sharing of lessons learned between nations at risks can generate potential to improve disaster preparedness in order reduce impacts on the food supply.

Two examples of lessons learned are given from the past disaster impacts on critical infrastructure of the food supply: Queensland Flood, Australia and Hurricane Sandy, the United States. These represent only an extract of lessons learned from these two past disasters.

Lessons from the Queensland Floods (Australia)

The food industry is a main part of the Australian economy. Therefore the Australian food supply is an essential element of the national infrastructure (CIP). As described before, the Queensland floods had major impacts on the food supply. "The perception among not only state authorities but also, in retrospect, major food retailers was that the northern parts of Queensland had insufficient warehouse capacity to meet demand (of food shortages and disruption)" (Queensland Floods Commission of Inquiry 2012: 32). Thus one of the main lessons learned is the "backup or contingency planning, […] stocks of some essential food and grocery items, and […] established relationships with suppliers who can include […] stores in their own contingency planning" (Queensland Floods Commission of Inquiry 2012: 32).

Lessons from Hurricane Sandy (USA)

The impacts of Hurricane Sandy on the food supply were locally bounded. The private food sector immediately returned to routine operations after the power supply was repaired. Due to the main responsibility of the private food sector approach, no further harmful food supply disruption were recorded. Furthermore the Federal Emergency Management Agency (FEMA) gives recommendations to individuals and households to be self-sufficient for at least three days (self-sufficient with food and water items for up to 14 days is recommended). Many residents "who failed to evacuate did not have enough supplies on hand to survive" (Bucci et al. 2013: 7). That shows the importance of preparedness on the individual and household level to deal with hazardous events and disasters. Efforts were taken after Hurricane Sandy to improve and engage preparedness on this level.

3.2 Disruption of the Critical Infrastructure Food: Impact on the Population

Ensuring the Food Supply during disasters seems to be essential with regard to the population's well-being. On the one hand, it seems to be important to ensure the

Food Supply and Security to safeguard the populations' physical health (e.g. need to have access to food and hygiene). On the other hand it assumes to be necessary to ensure the Food Supply to guarantee the public security and safety and to prevent hoardings.

3.2.1 Household Preparedness

To minimize the impacts of possible threats, some of the OECD member countries implemented a strategy to prepare the population in case of a disaster. Although some of the countries like New Zealand, Australia or the United States hold different guidelines, the main aim has the same intention: being prepared can help to reduce impacts on individuals and households. Hence New Zealand, Australia and the United States serve as examples to present different ways of being prepared at the household level. Table 3 shows different communication and education statements, different emergency preparedness recommendations as well as emergency kits items.

- Communication and Education: Mission statement of emergency preparedness and disaster management strategies of the selected countries
- Emergency preparedness: recommendations of involved stakeholders for households to be self-sufficient
- Emergency kit: recommended items of food and water supplies.

Table 3 Household preparedness in different OECD countries

Country	Communication and education	Emergency preparedness	Emergency kit (examples)
New Zealand	"Get Ready Get Thru, Shake Out"	Self-sufficient for up to 3 days	• Food, formula and drinks for babies and small children • Non-perishable food (canned or dried food)
Australia	"Be prepared"	• Ready to be self-sufficient for at least 3 days in case of leaving home • Self-sufficient for up to 14 days	• Pet food • Snack food • Ready-to-eat canned or bottled food • Dried and long-life food • Drinks
United States	• "Are you ready?" • "Ready: Prepare, Plan, Stay informed"	• Self-sufficient for up to 14 days • Ready to be self-sufficient for at least 3 days	• Special dietary needs • Stock canned foods, dry mixes, and other staples that do not require refrigeration, cooking, water, or special preparation • Salt-free crackers, whole grain cereals, and canned foods with high liquid content

Sources Civil Defence Emergency Management (2015), Australian Red Cross (2009), Federal Emergency Management Agency (2004)

Campaigns like "Get Ready Get Thru, Shake Out" of New Zealand encourages households to take action and to be prepared in case of disasters to minimize the impacts to their household. Different tools and media are used within the countries to catch the household attention to help to be prepared for different hazards. There are several online resources to download checklists or fact sheets. For instance household emergency plans serve as checklists to ensure a high level of preparedness with food supplies. Long-life and dried food are the most important food items which can be found on the emergency kit checklist of all three countries. Furthermore there are videos explaining how to prepare an emergency kit and which circumstances of different hazards have to be considered. Another aspect relating to prepare individuals and households in case of disasters is addressing different vulnerable groups with special information of food supply items. The Australian Red Cross, for example, published an emergency plan for people with a disability, their families and care givers. Furthermore they published an emergency plan for seniors. Vulnerable people have to check their needs and capabilities (e.g. allergies or sensitivities (food, drugs etc.) with a personal assessment worksheet.

In conclusion, emergency preparedness on the household level is a way to reduce impacts of possible threats and during disasters situations affecting the food supply.

4 Conclusion

If a disaster occurs, the critical infrastructure of the food supply can be severely affected. Different types of hazards (natural as well as man-made) can have impacts like disruption of the food supply for the population.

Countries like Australia, New Zealand or the United States involve the population in preparing their households with food items. Recommendations to hold a supply to be self-sufficient for up to 3–14 days are recommended. Learning from past disasters on the one hand and preparing households to be self-sufficient for up to 3 days on the other hand are essential steps to reduce vulnerability in critical infrastructures during crises and large scale disasters. Disruption of the food supply during Hurricane Sandy showed how important stocks at the household level are key enablers to resilience.

Beyond referring to Food as CI, it became apparent that ensuring the Food Supply in crisis situations appears to be essential with regard to the population's well-being. It is essential to ensure the Food Supply and Security to safeguard the populations' physical health (e.g. need to have access to food and hygiene). As well, it is important to ensure the Food Supply with regards to guaranteeing the public security and safety and to prevent actions such as hoarding and similar disturbances in crisis and disaster situations. Inferences can be drawn from contemplating the interdependencies of the Food sector about the character of the populations living and what the community members depend upon (Masys 2014: 266). Food as critical infrastructure (including the food supply and safety) implies various impacts on the civil security. Considering this, Collier and Lakoff (2008: 1) summarize: “In recent years “critical infrastructure protection” has emerged as an increasingly important framework for understanding and mitigating threats to security.” In the new “global security environment” it is essential to be continually mindful of unknown, new and emerging risks.

References

Australian Red Cross (ed) (2009) Emergency REDiPlan Four steps to prepare your household. Australian Red Cross, Carlton, Victoria 2009

Authority of the Minister of Health (eds) (2007) Emergency food service: planning for disasters. Centre for Emergency Preparedness and Response. Ontario/Winnipeg

Blanchard BW (2008) Guide to emergency management and related terms, definitions, concepts, acronyms, organizations, programs, guidance, executive orders & legislation. [Online] Available https://training.fema.gov/hiedu/docs/terms%20and%20definitions/terms%20and%20definitions.pdf. Accessed 26 Oct 2015

Bryant E (2005) Natural hazards. Cambridge University Press, New York

Bucci SP, Inserra D, Lesser J, Mayer MA, Slattery B, Spencer J, Tubb K (2013) After hurricane sandy: time to learn and implement the lessons in preparedness, response and resilience. Special Report from the Heritage Foundation Emergency Preparedness Working Group. Special Report No. 144. Washington

Civil Defence Emergency Management (eds) (2015) Get ready. Get Thru. [Online]. Available http://www.getthru.govt.nz/how-to-get-ready. Accessed 12 Jul 2015

Collier SJ, Lakoff A (2008) The vulnerability of vital systems: how “Critical Infrastructure”-became a security problem. Dissertation

Commonwealth of Australia (eds) (2011) Resilience in the Australian food supply chain, Australian Government. Department of Agriculture, Fisheries and Forestry. Australian Government

Deutsches Komitee Katastrophenvorsorge eV (eds) (2004) Lessons Learned. Schriftenreihe des DKKV, no. 29. Lernen aus der Katastrophe 2002 im Elbegebiet. Hochwasservorsorge in Deutschland. tsches Komitee für Katastrophenvorsorge e. V. (DKKV). Bonn, 2004

Dun & Bradstreet (eds) (2011) Report: mitigating supply chain risks [Online]. Available http://www.dnb.com/content/dam/english/business-trends/mitigating_supply_chain_risk.pdf. Accessed 13 Jul 2015

Federal Office for Information Security and Federal Office of Civil Protection and Disaster Assistance (eds) (2013) Critical infrastructures [Online]. Available http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html. Accessed 12 Jul 2015

Federal Republic of Germany (eds) (2009) National strategy for critical infrastructure protection (CIP Strategy). Federal Republic of Germany. Berlin

FEMA—Federal Emergency Management Agency (eds) (2004) Food and water in an emergency. FEMA. Jessup, Maryland

Government of British Columbia (eds) (2006) Emergency social services [Online]. Available http://www2.gov.bc.ca/gov/content/safety/emergency-preparedness-response-recovery/volunteers/emergency-social-services#what. Accessed 26 Oct 2015

Government of Netherlands (eds) (2015) Protecting critical infrastructure [Online]. Available http://www.government.nl/issues/crisis-national-security-and-terrorism/protecting-critical-infrastructure. Accessed 29 Jul 2015

Harris A (2015) Food supply continuity. Department of Primary Industries. Victoria. [Online]. Available https://ehpa.org.au/download/Symposium%20Preceedings/2012_symposium_-_thursday/David%20Harris-2.pdf. Accessed 26 Oct 2015

Homeland Security (ed) (2013) National infrastructure protection plan (NIPP): partnering for critical infrastructure security and resilience. Homeland Security, Washington

Kuhlicke C, Kabisch S, Krellenberg K, Steinführer A (2012) Urban vulnerability under conditions of global environmental change: conceptual reflections and empirical examples from growing and shrinking cities. In: Kabisch S, Kunath A, Schweizer-Ries P, Steinfuhrer A (2012) Vulnerability, risks and complexity. Impacts of global change on human habitats. Advances in people-environment studies, vol 3. Hogrefe Publishing. Cambridge/Göttingen, pp 27–39

Kirchner E, Fanoulis E, Dorussen H (2012) An analysis of civil security systems in the UK and Ireland. University Association for Contemporary European Studies (UACES) annual Conference, Passau, Germany, 2–5 Sept 2012

Masys AJ (2014) Critical infrastructure and vulnerability: a relational analysis through actor network theory. In: Masys AJ (ed) Networks and network analysis for defence and security. Springer, Berlin, pp 265–280

Ministry of Defence (eds) (2011) Security strategy for society. Ministry of Defense, Helsinki (Finland)

OECD—Organisation for Economic Co-operation and Development (eds) (2008) Protection of critical infrastructure and the role of investment politics relating to national security. Investment Division, Directorate for Financial and Enterprise Affairs Organisation for Economic Cooperation and Development, Paris

Queensland Floods Commission of Inquiry (eds) (2012) Queensland floods commission of inquiry. Final report. Brisbane

Ridley G (2011) National security as a corporate social responsibility. Critical infrastructure resilience. J Bus Ethics 103(1):111–125. (Springer Netherlands, 2011)

Rueckversicherungs-Gesellschaft M (2015) Naturkatastrophen 2014. Analysen, Bewertungen, Positionen. Ausgabe 2015. Münchener Rückversicherungs-Gesellschaft. München, 2015

Swedish Institute of International Affairs (eds) (2014) Civil security and the European union. Swedish Institute of International Affairs, Stockholm

The White House. Office of the Press Secretary (eds) (2014) Presidential Proclamation—critical infrastructure security and resilience month [Online]. Available https://www.whitehouse.gov/the-press-office/2014/10/31/presidential-proclamation-critical-infrastructure-security-and-resilienc. Accessed 26 Oct 2015

Thywissen K (2006) Components of risk. A comparative glossary. In: Studies of the University: Research, Counsel, Education Publication Series of United Nations University Institute for Environment and Human Security. No. 2/2006. United Nations University Institute for Environment and Human Security

Trusted Information Sharing Network for Critical Infrastructure Protection (eds) (2012) Enhancing the safety and security of our food supply. The NETWORK, Commonwealth of Australia

UNISDR—United Nations National Strategy for Disaster Reduction (eds) (2009) Terminology on disaster risk reduction. United Nations International Strategy for Disaster Reduction. UNISDR, Geneva

UNISDR—United Nations National Strategy for Disaster Reduction (eds) (2011) National strategy for disaster reduction. Themes and issues in disaster risk reduction [Online]. Available http://www.preventionweb.net/files/23647_themesandissuesindisasterriskreduct.pdf. Accessed 01 Jul 2015

Zimmermann R, Restrepo CE (2009) Analyzing cascading effects within infrastructure sectors for consequence reduction. In: International conference on technologies for homeland security, Waltham

The Role of Social Network Sites in Security Risks and Crises: The Information Warfare of Terrorism

Ken Wewa-Wekesa

Abstract Social Network Sites (SNS) have in recent years received significant universal attention in the way they have changed lives socially, politically and economically through distinct components that enable people from all over the world to connect instantly. This work analyses the aggressive nature in which terrorists quickly adapt to these SNS vis-à-vis governments' approach to risk communication and situational crisis communication using the same media. It additionally examines literature on the publics' cumulative behaviour regarding the use of SNS in the context of terror attacks and the terrorists' use of the same media to coordinate their operations in recruiting people to join their organisations, planning and execution of terror attacks. To achieve that, this chapter investigates the online cumulative behaviour which has been witnessed recently (e.g. during the Westgate Mall attack by Al-Shabaab in Nairobi, Kenya in 2013) and the terrorists taking advantage of these platforms [e.g. the Islamic State of Iraq and Syria (ISIS)] to stimulate crises of national security.

Keywords SNS · Terrorism · ISIS · Al-Shabaab

1 Introduction

> Democratic nations must try to find ways to starve the terrorist and the hijacker of the oxygen of publicity on which they depend.
>
> Margaret Thatcher, 1985

The above proclamation was made by the late former British Prime Minister, in the aftermath of the Trans World Airlines hijacking (New York Times 1985). It is emblematic of the dynamic challenges faced by authorities in the Global War on Terrorism, in relation to the media. At the time this statement was made, it was hardly envisaged that there would come a time when a creation of advanced

K. Wewa-Wekesa (✉)
University of Leicester, Leicester, UK
e-mail: ken.wekesa@gmail.com

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_14

web-based internet applications—known as “web 2.0” (O’Reilly 2007: 17)—would allow terrorists to exchange ideas, images and share information in a way that is nearly unregulated. These internet-based applications that aid the creation and sharing of user generated content have come to be commonly referred to as SNS.

The development of this “web 2.0” technology has aided the emergence of a network with a universal reach, and comparatively reduced obstacles to entry, thereby creating challenges in the fight against terrorism. According to the latest figures by Communications Authority of Kenya (CA), over 70 % of Kenyans have internet access, owing largely to a meteoric rise in mobile data subscriptions (CA 2015: 23). As many people embrace internet technologies for profitable opportunities, so have terrorist organizations taken advantage to exploit them for deleterious ends.

This research revealed how terrorists have skillfully adopted SNS in their strategic operations to interact with their colleagues and the general public. Furthermore, the study revealed a depth of nescience amongst some members of the public, regarding the use of SNS during a crisis caused by a terror attack. This research also revealed that as much as some people view SNS with a lot of optimism, some security experts and counter terrorism analysts believe that these new technologies have brought about extensive challenges in terms of countering terrorism covert operations and propaganda.

A practical approach has been adopted with regard to categorization of the ways by which SNS is often used to aid and abet acts of terrorism. This resulted in the identification of three categories: Propaganda, planning and execution. Propaganda focuses on incitement, recruitment and radicalization; planning analyses terrorists’ covert communications, while execution discusses the ways in which these tools help terrorists to launch attacks.

2 Historical Background

Terrorists’ affection for media attention has been a perennial obsession. In an effort to advance their agenda to the masses, both terrorists and governments engage in a tug of war for publicity, with the media being in the loop of public attention, as to what angle they adopt in reporting information received. As regulators of communications within specific borders, governments sometimes deny terrorists a platform of publicity by prevailing upon the media not to relay information deemed to be damaging. In examining this objective, Entman (2004) describes a media framing model referred to as the cascade model, which elaborates the relationship between the White House and the media and ultimately how the White House’s agenda is reported to the public. He projects the White House’s power plays that involve four elements: power, cultural congruence, motivation and strategy, all of which interact to push through their propaganda. On the other hand, perpetrators of terrorist activities have for many years realized that they can easily be muzzled by government-controlled media and can only get press coverage if they stage ‘an attention-grabbing incident’ or they launch an attack where global events are taking place. Such events are their favorite targets because they are guaranteed automatic publicity owing to the ready huge media personnel on site (Perl 1997).

To demonstrate how serious they take their agenda, Perl (1997) enumerates benefits that terrorists hope to gain from media coverage. One of them is publicity which draws the world's attention to the existing problems. Secondly, through publicity, they hope the public would empathize with their cause. The third objective that they seek is for the media to legitimize their cause so that it looks genuine in the court of public opinion. The fourth importance they attach to coverage is in a hostage situation where media unravels plans of governments' retaliation which enables them to come up with counter strategies and finally they use the media to hurt the enemy by spreading propaganda that would cause fear and heighten panic amongst the populace. While governments' intentions are to systematically reverse these expectations, they are faced with the challenge of delivering timely communication to assuage fear which is per se, considered a risk to people's health (Gray and Ropeik 2002). The emphasis of this timeliness is reflected in the media folklore as a golden opportunity, with the complementary maxim "old news is no news" (Perl 1997).

3 Objective of the Study

The overall aim of this study was to analyze SNS used by terrorists, the public and governments in relation to security issues by asking: "What is right with SNS and what is wrong with them in relation to terrorism?" This broadly helps to explain the risk and crisis discourse vis-à-vis terrorism. Particularly, it explored the perceptions of public users of SNS, security experts and government authorities and how it impacted on intelligence gathering and security.

Applying crisis communication literature, this study examined how the public users of SNS understand their moral role in security matters and how the government reacts to the threat posed by terrorists' SNS communication. In addition, risk communication literature was analyzed with a particular focus on how effectively governments communicate risk to the public using SNS.

Using qualitative methods, this study employed in-depth interviews with members of the public who are active users and consumers of SNS, journalists, bloggers, public relations experts, security experts, digital content experts and CA officials to examine their perceptions on the dissemination, interpretation and regulation of SNS news content as well as censorship of the same with regards to terrorists. Particularly, this study explored risk communication theory as conceived by Irwin (1995) and Situational Crisis Communication Theory as defined by Coombs (2007) against the backdrop of challenges faced by authorities in regulation and response to SNS applications such as Twitter, Facebook and WhatsApp in fighting terrorists' activity and their agenda. The analysis shows that these web applications have enhanced terrorists' opportunities to execute their goals.

4 SNS and Terrorism

The literature regarding SNS and terrorism is ever growing in great proportions. It is important to elaborate how communication dynamics have changed with the emergence of SNS. In the course of studying the impact of crisis communication medium, message content, secondary crisis communication and secondary crisis response, Schultz et al. (2011) postulate that the channel of communication is more important than the message. In the context of crisis in general, this research seems to exalt the importance of social media as it goes ahead to point out that Twitter is a vital and influential tool in crisis response.

SNS are not new to communication. The first social network site—SixDegrees.com—was launched in 1997 (Dewing 2012). Since then, a multitude of SNS have sprung up, attracting hundreds of millions of users. The advent of SNS revolutionized the way news is relayed and subsequently the way organizations, governments and the public interact. Freberg and Palenchar (2013) argue that SNS coupled with strategic risk and crisis communication provide a thriving scope for communication research and practice. In fact, "formal guidance about using SNS in professional codes and guidelines created by strategic communication organizations is still in its developmental stage" (Stewart and Coleman 2013: 182).

According to Fox and Gangl (2011) eight vital features have made SNS a game changer in comparison to traditional media: The first is anonymity, (where users deliberately use aliases in lieu of their real names) which has provided an opportunity for people to comment on sensitive issues whilst evading responsibility. Secondly, users are afforded the luxury of divergent sources for their news (e.g. Facebook, Twitter, Youtube, Blogs), and can be relied upon simultaneously. Thirdly, the omnipresence of SNS is such that the lives of the elite, powerful and influential figures of the society are under the public microscope and anyone can record their "private" activities and make them public. The fourth alteration is the speed with which news and information is shared to the masses and the fact that the information reaching people may be unconfirmed. The fifth attribute is that it has broken down barriers of hierarchies, which means that relationships among users are undefined. This is unlike in traditional media where reporters have a clear channel of filing their reports and editors have the final say. The sixth feature is the shift from being objective to being subjective. Many users do not feel any obligation to be objective on anything they report but they are mostly motivated by their inclinations to different things. The seventh modification is the capacity to merge textual, audio and visual representations with a lot of ease. For instance, one is able to combine a text and an image or with a video and disseminate as one package. The final trait of SNS is the dearth of regulation or censorship which is common with traditional media.

Terrorists are not new to cyberspace. Scholars have parsed and analyzed various aspects of this topic but they don't seem to agree on how to categorize diverse forms of cyber-related crimes. Denning (2010) suggests that the term cyber-terrorism was used for the first time by Barry Collin in 1982 to imply the confluence of the cyber and the physical world. This narrative goes as far as forecasting how terrorists would launch a cyber attack against crucial infrastructure. The discourse on terrorism and cyberspace is too murky because of the different interpretation of the phrase ‘cyber-terrorism’ by different scholars. While Denning (2000) holds that cyber-terrorism is an assault which employs a programmable electronic device such as a computer to wage war against an enemy, Bronskill (2001) argues that the phrase entails internet propaganda and online recruitment. Although a lot of attention has been directed towards cyber-terrorism debate in the last few years, that subject is beyond the scope of this research and consequently was not part of examination.

The shift from online chat forums to SNS was a watershed moment for terrorist organizations. In recent years, several militant groups—Somalia based Al-Shabaab, Syrian based Jabhat al-Nusra, Tehkreek-e-Taliban Pakistan (TTP), Al Qaeda in the Islamic Magreb (AQIM)—have all either taken to Twitter or Facebook with thousands of followers and have been actively spreading and selling their agenda to the masses along the lines of ‘social network site Jihadis’ (CNN 2013). Other groups like ISIS have employed extra strategies such as instant messaging services like WhatsApp to communicate discretely and plan their atrocious operations within their common network. In view of these developments, it is imperative to examine these SNS in ways that they enhance terrorists’ activities.

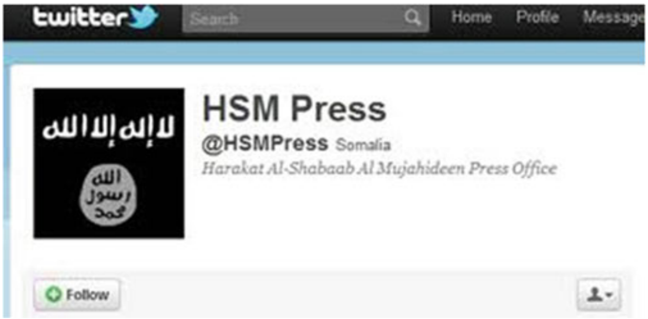
4.1 SNS and Their Influence on Terrorism

Facebook: Founded in 2004, this is currently the most popular social network site, available in 37 different languages around the world—with over one billion monthly active users—that permits registered users to create profiles, post statements on timelines, upload photos, recorded video clips, send messages and keep in touch with “friends” (Facebook, undated). The site has attractive features such as: Timeline, which is a space on the profile page that enables one to display their posts as well as view posts from friends; “Like” button which is a feature that is symbolic of an “endorsement” of contents or statement and “Share” button, which is a feature that enables subscribers to distribute widely a post or content to other subscribers (Facebook, undated). The speed at which a particular news or image is shared on SNS, the amount of shares and the reach qualifies the content to be labelled as “viral” (Nahon and Hemsley 2013).

Facebook has over five million subscribers in Kenya (Business Daily 2015), it is claimed that two young Kenyan women arrested by police while crossing into Somalia to join Al-Shabaab militants were recruited through Facebook (Standard Digital 2015). The New Statesman (2013) illustrates the apparent audacity demonstrated by TTP in an advertised message posted on Umar Media, their Facebook page, which sought to hire specialists in the production of their media content. The message which was laden with belligerent connotations read “Dear brothers and sisters, ‘the pen is mightier than the sword’. Now you have a chance to use this mighty weapon”. They brazenly posted the email address to those interested in the ‘job opportunities.’ Although Facebook later shut down the page, TTP opened a new page almost immediately which rapidly received thousands of “likes”.

Twitter: Launched in 2006, Twitter is a microblogging site that allows its users to send images and alpha-numeric messages up to 140 characters long to a list of followers (PC Mag 2015). Twitter has been used as a communication and propaganda tool especially by Al-Shabaab. With an astounding 500 million tweets per day Twitter is the fastest growing social platform in the world (GlobalWebIndex 2013; Telegraph 2013). Kenya is ranked second in Africa—behind South Africa—in terms of Twitter-active countries. Statistics also indicate that most twitter users in Africa are below 30 years old. While the global average age of Twitter users is 39 years, 60 % of Africa’s users are aged between 21, 29 and 57 % use Twitter from their cell phones (Portland Communications 2012).

Al Jazeera (2013a) claims that the Al-Qaeda affiliate joined Twitter on December 7, 2011 in a reactive measure to counter Kenyan military spokesman Major Emmanuel Chirchir’s Twitter account, which was launched to highlight the Kenyan forces’ success in the midst of the invasion of the Shabaab-occupied Southern Somalia. Al-shabaab’s first Twitter handle was created with a typically Islamic visage, complete with an uploaded Arabic avatar, designated as @HSMPress which are the initials for Harakat Al-Shabaab Al-Mujahideen, translated to “Mujahideen Youth Movement”.

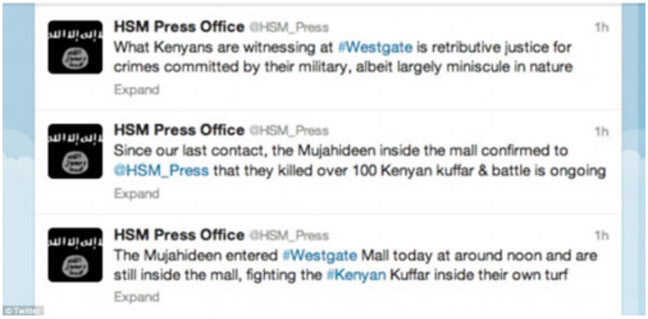


HSM Press
@HSMPress Somalia
Harakat Al-Shabaab Al Mujahideen Press Office

Source @Twitter (2013)

After using the account to tweet a series of savage messages, posting graphic photos of a French soldier they killed and threatening Kenyan hostages, Twitter closed down the account in January 2013. This action saw the reincarnation of Al-Shabaab with a new account a few days later (Los Angeles Times 2013a, b). The group has been engaging Twitter in a hide-and-seek game in which they have been desperately seeking to have a presence on the social media platform with several mutated accounts such as @HSMPress1, @HSM_Press, @HSM_PressOffice, @HSM_PR, @HSMPress_arabic, and @HSM_PRESS2. All these accounts have been used by the militants when Twitter executes one suspension after the other, disguising itself with different handles albeit with the same Twitter interface and avatar to retain its identity.

The attack on the Westgate Mall in Nairobi, Kenya, on September 21, 2013 demonstrated the modern-day social media edification of Al-Shabaab communication system. By live-tweeting the events of the siege that lasted for four days and left more than 65 people dead, they were certain that the whole world was following their timeline and were convinced that their sentiments, cause and demands would be conveyed to a worldwide audience. In order to maintain a personal touch with their followers, they referred to the attackers inside the mall as the "Mujahideen" (warriors) while labelling the hostages as the "Kuffar", an immensely disparaging term for non-Muslims.



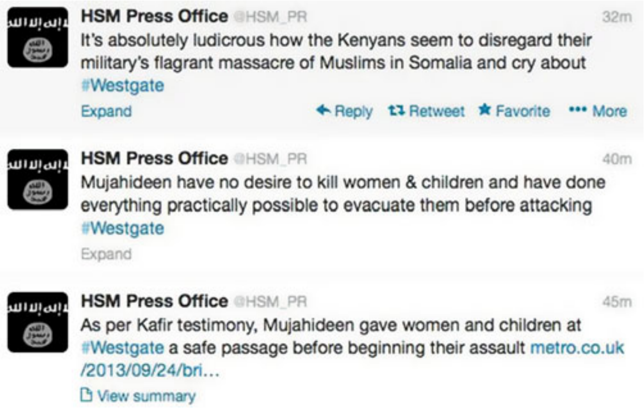
HSM Press Office @HSM_Press 1h
What Kenyans are witnessing at #Westgate is retributive justice for crimes committed by their military, albeit largely miniscule in nature

HSM Press Office @HSM_Press 1h
Since our last contact, the Mujahideen inside the mall confirmed to @HSM_Press that they killed over 100 Kenyan kuffar & battle is ongoing

HSM Press Office @HSM_Press 1h
The Mujahideen entered #Westgate Mall today at around noon and are still inside the mall, fighting the #Kenyan Kuffar inside their own turf

Source @Twitter (2013)

Showcasing their avid use of Twitter, they tweeted messages gloating about the siege, taunting the Kenyan security forces, attempting to sway the public mood in their favor with propaganda on how best the hostage situation could have been avoided and how kind they were to have had mercy on women and children. All this spin to win the hearts and minds of the Kenyan public put their canny use of the platform into perspective.



HSM Press Office @HSM_PR 32m
It's absolutely ludicrous how the Kenyans seem to disregard their military's flagrant massacre of Muslims in Somalia and cry about #Westgate

HSM Press Office @HSM_PR 40m
Mujahideen have no desire to kill women & children and have done everything practically possible to evacuate them before attacking #Westgate

HSM Press Office @HSM_PR 45m
As per Kafir testimony, Mujahideen gave women and children at #Westgate a safe passage before beginning their assault metro.co.uk/2013/09/24/bri…

Source @Twitter (2013)

These tweets offered free flowing coverage to both local and international media who could not cover the events inside the mall first-hand, the public, security and intelligence experts as well as the sympathizers of Al-Shabaab. This was in stark contrast to Kenyan government officials who seemed to have been caught napping as they gave contradictory information both in live press conferences and Twitter (Al Jazeera 2013b). To back up Kenya's fight against Al-shabaab, Twitter "verified"—marked with a blue badge to establish authenticity—all government's officials' accounts reporting on the siege. Despite this, there was still communication of contradictory messages to the public from Kenya's interior cabinet secretary Joseph Ole Lenku, Foreign affairs cabinet secretary Amina Mohamed, Kenya police and the military. These disparities from the government's accounts ranged from the number of attackers who stormed the mall to, the number of casualties and the mystery of whether there were any women amongst the terrorists.

"…Foreign Minister Amina Mohamed told PBS that a British woman and two or three Americans were among the terrorists, but Interior Minister Joseph Ole Lenku earlier said no women were involved" (Los Angeles Times 2013b). Sky News (2013) reported the account of security sources directly involved in the operation saying that some of the explosions heard inside the mall were set off by Kenyan forces but this was also contradicted. "Security officials at the scene said the explosions had been caused by Kenyan forces who set off blasts to get in through the roof. However, Mr Lenku said the smoke had been down to the Al-Shabaab fighters setting fire to mattresses as a decoy" (Sky News 2013). Such conflicting messages stirred anger amongst Kenyans who felt that the government was quickly losing credibility at a time that the whole country needed reassurance to restore confidence.

WhatsApp: Founded in 2009, this is a mobile messaging application which works across all phone and web-based platforms and allows users to send each other messages without having to pay for them since it uses the same internet data for web browsing (WhatsApp, undated). According to Business Insider (2015) FBI assistant director Michael Steinbach, while attending a congressional hearing, bemoaned the use of strong encryption technology that is creating "dark spaces" and grants terrorists "a free zone by which to recruit, radicalize, plot and plan". The Guardian claims that WhatsApp uses default end-to-end encryption with the aim of preventing sleuths from hacking into its system and snooping on users' communications: "The TextSecure encryption protocol is particularly strong as it uses a form of what's known as "forward secrecy", which means a fresh key is created for every message sent" (Guardian 2014). The Daily Mail (2015) avers that most of the encryption services were conceived in the wake of Snowden's revelations on the ability of British and US intelligence organisations to spy on people's internet histories, emails, text messages, call records and passwords.

4.2 To Shut or not to Shut?

In the midst of social media popularity, there has been frenzied debate amongst policy makers, intelligence community, counter terrorism experts, media stakeholders and government security agencies on whether terrorists should continue being allowed the freedom to use the platform to further their agenda.

The World Economic Forum (WEF 2013) postulates that in our hyperconnected world, these "Digital Wildfires" tend to have incorrigible attributes especially in highly explosive circumstances, because inaccurate information relayed to the masses can cause devastation before the possibility of correcting the information. Simon et al. (2014) recount a typical example of misinformation that made rounds on Twitter during the Westgate mall attack: "During the first day of the attack, two unique tweets were posted, claiming to show pictures of the attackers. These messages were retreated 106 times, 81 of them within 30 min…. These pictures were not of the attackers but rather of the Kenyan armed forces. The photos were removed after approximately two days". WEF states that a lot of things can go wrong in cases where facts are misrepresented: "The real-world equivalent is shouting "fire!" in a crowded theatre—even if it takes only a minute or two for realization to spread that there is no fire, in that time people may already have been crushed to death in a scramble for the exit" (WEF 2013).

Whilst most governments and anti-terrorism policy makers advocate for known terrorist accounts to be shut down, independent analysts tend to take a more cautious view as they reckon these accounts may prove helpful in some instances. Addressing an International Conference on Cyber Security at Fordham University, on August 4, 2010, security expert Evan Kohlmann, gave a chilling narrative reflecting on the time bomb that is the social networking sites (Kohlmann 2010) Not only do they offer anonymity, interactivity and a resilient structure that terrorists thrive upon but also more importantly, a large followership may unwittingly encourage some people amongst those who are less likely suspected to be 'lone wolves'. Kohlmann (2010) describes how in 2009, a young Jordanian medical doctor, Humam al-Balawi—his *nom de guerre*, Abu Dujana al-Khorasani—was recruited from a social network site by the country's intelligence agency, in collaboration with the US Central Intelligence Agency (CIA), to infiltrate Al-Qaeda's top ranks in Afghanistan but despite having no previous links to terrorist networks, volunteered as a suicide bomber on behalf of the terrorist group, killing seven CIA agents in Afghanistan. This is one of the illustrations that demonstrate how lone wolves can be nurtured within social media sites and pose unpredictable danger to the society.

A comparison of user policies gives a clear picture of how the two popular social media sites deal with this prevalent menace. Under the rules found on its website, Twitter states "We respect the ownership of the content that users share and each user is responsible for the content he or she provides. Because of these principles, we do not actively monitor and will not censor user content…." (Twitter, undated). While they actually, take steps to crack down on offenders, the fact that they make it clear that they do not "actively monitor" and "will not censor user content" may be sending a wrong message to those who are keen on seeing strict regulation. Unlike Twitter, Facebook is more assertive with direct mention of those who are barred from using their service. "Organizations with a record of terrorist or violent criminal activity are not allowed to maintain a presence on our site" (Facebook, undated).

Social media and terrorism commentator, Aaron Zelin, cited by Radio Free Europe (2013) dismisses the idea of gagging terrorists on social media as a futile move as it is practically impossible to monitor every single account: "It creates a situation where it's like 'whack-a-mole,' where something will go offline but then it will create a new account and it will stay online for a little while, and then will be taken offline again and so it's this cat-and-mouse-type game". This explains why Twitter has suspended more than seven Al-Shabaab accounts but they keep resurfacing with a new account at every opportunity.

Gertz (2013) posits that most intelligence agencies are wary of kicking out terrorists from social media. The agencies constantly monitor their friends, followers and location and thus, shutting them down would be counterproductive to their efforts to keep tabs on terrorist activities. Berger (2013a) disagrees with this notion and makes three arguments for them to be regulated or completely blacked out: Firstly, that no valuable intelligence information can be gathered from these Twitter accounts because they only use the platforms to "harass, annoy and threaten". Secondly, that there are many other 'better' sources of intelligence online than social network accounts, and finally the argument of letting them operate freely owing to freedom of speech is disqualified on the basis of terrorists' threats of violence that do not deserve protection. He particularly castigates Twitter for having lax policies against terrorists and general violent content posted on its site and being slow to act despite numerous reports of violations. "Designated terrorist groups still use Facebook and YouTube, but they don't maintain official accounts over long periods of time because Facebook and YouTube don't allow it. Twitter makes it easy, so that's where you find the official terrorists" (Berger 2013b). The fact that terrorist organizations are getting more adroit at using modern media technology better than most governments is not lost on even the most developed nations in the world. Former US Secretary of Defense Robert Gates stated "It is just plain embarrassing that Al Qaeda is better at communicating its message on the internet than America" (cited in New York Times 2007).

5 Theoretical Framework

Every terrorist attack presents varying situational, emotional and psychological demands in the general public that impact on how information is delivered and how governments attempt to manage the crisis. Following the overwhelming use of SNS by terrorists, there have been extensive debates both in academia and among commentators with regards to how SNS affect governments' counter terrorism efforts. Consequently, the rise of mobile phones and related technologies has reshaped the complex matrix of communication and social interaction. Wright and Hinson (2009) claim that these SNS platforms are popular owing to their modest cost or unpaid services and thus provide numerous opportunities to exchange information and new channels for universal outreach.

This study employed theories that have previously examined risk and crisis communication and provides a link between terrorists, publics and governments. These theories are explored from the lens of informing the public about terrorism-related risks and responding to crisis in the age of SNS. In this section, the word ‘organization(s)’ has been predominantly used vis-à-vis risk and crisis communication because previous studies have made organizational risk and crisis the focal point. Nonetheless, in this study, the word ‘organization (s)’ or ‘institution(s)’ exemplifies ‘government(s)’ both in structure, operations and reaction to risk and crisis.

5.1 Risk Communication

The public is generally shaped by risk communication in unanticipated ways. The conceptual templates on risk communication are important from one subject area to another. In his renowned publication, the risk society, Beck (1992) argues that the society seems to be shifting from acquiring things that would protect them from risks towards avoiding the things that expose them from risks, a situation which has been spurred by media’s preoccupation with risk conflicts. Irwin (1995) holds that most communication strategies are hinged on deficient models that presume that the public who are vulnerable to risk, have a paucity of knowledge on risk and therefore more information relayed to them will not be useful. Borodzicz (1996) views risk communication as a series of actions replete with moral dilemmas. He claims that any attempts to come up with practical objectives for people with disparate expectations may amplify hostilities.

National Research Council (1989) asserts that risk communication ought to be bi-directional involving the entity that relays the information and the public who are the targeted consumers of risk information. For risk communication to be efficient, Fischhoff (2002) advises that the communicator of the message must first understand what the recipient believes so as to inspire them to espouse behavioral change. Governments, in some cases, have a dim view of communicating certain aspects of risks to the public and tend to either conceal information or give the bare minimum which may end up creating a perception of isolating the public. Wales and Mythen (2002) point out that the UK government has on numerous occasions mishandled its communication to the public and as a result created an atmosphere of distrust. In cases where there is distrust, people are inclined to perceive some risks as bigger or lose faith in those charged with formulating policies (Rogers et al. 2007). Similarly, it is not disputable that the media’s magnification of some issues aid in agenda setting, and as a result, heightens or reduces the perception of risk in the society (Kasperson and Kasperson 1996).

In relation to terrorism, Fischhoff (2006) enumerates three pertinent criteria to make risk communication successful: from the outset, risk should be managed well in order to have conceivable information to relay; this should be followed by the creation of suitable channels to build public credibility by showing that plans are supported by preparedness and recovery; and finally, it is imperative to transmit information that is relevant and accurate by analyzing what is within the public knowledge and then create a message that will compliment what is lacking. These standards are echoed by Kasperson and Palmlund (2005) who emphasize that those tasked with communicating risk must produce a great equilibrium between relaying truthful, beneficial information on risk and eschewing anything that causes unwarranted apprehension.

The application of SNS to risk communication is scanty owing to claims that SNS give rise to rumours, misinformation and public anxiety. In fact, some scholars who are cynical of SNS posit that "while traditional media (newspapers, radio) seem to both attenuate and amplify risk perceptions, digital media, including electronic technologies (blogs, podcasts, wikis, etc.) generally tend to amplify risk perceptions. Digital media are seldom subject to editorial oversight and generally focus on the "spectacular", even if the claim is objectively and scientifically indefensible" (Berube et al. 2010: 9). Other authors point out that SNS have advantages in risk communication, stating that owing to the subdivision of social categories on the internet, appropriate groups of people can be targeted accurately. Strecher et al. (1999) argue that interactive media can be employed to adapt risk communication to suit users' risk perception, socio-cultural background, socio-demographic attributes and literacy standards.

5.2 *Crisis Communication*

Managing unpredictable situations is not a new dilemma, although the circumstance in which unpredictability happens has turned out to be more complicated. Since the events of September 11, 2001, many experts believed that there was a growing need for efficient crisis management. This has been emphasized by authors who believe that governments need to improve their approach to crisis response: "Terrorists want to create a crisis for governments. They do this by studying the response plans and designing scenarios that will test them and show them wanting. The need for a disciplined approach to crisis response needs to be dangerously balanced against flexibility" (Borodzicz 2005: 153).

A crisis exerts extreme pressure on an entity's physical, emotional and financial systems and could lead to the downfall of an organization (Pearson and Mitroff 1993). Coombs (1995) presents a strong theory in the field of crisis communication known as Situational Crisis Communication Theory (SCCT) which is a method for choosing crisis response strategies. This theory is comprised of three major concepts: crisis situation, crisis response strategy and a framework for harmonizing the crisis situation and the crisis response strategies. SCCT prescribes the selection of crisis response strategies that are suitable to the attributes of the crisis situation. It is also germane to point out that SCCT derived this connection from relationship management theory, neo-institutional theory and attribution theory. These theories are briefly examined below.

Relationship management theory—According to Ledingham and Bruning (1998) this theory explains the condition which prevails between an institution and its fundamental publics, in which action taken by any of the two entities, affect the political, cultural, economic and social welfare of either. Ledingham (2006) suggests that this theory moves the attention of message packaging, from communication towards relationships. In this regard, communication is used as a device for introducing, cultivating and sustaining the relationship between an institution and its stakeholders. Coombs (2000) holds that the history of a relation results to a certain reputation, both of which come from previous experiences between the institution and the stakeholders. He posits that those charged with managing crisis must envisage how their current relationship could impact on the stakeholders' perception of the crisis on the institution.

Neo-institutional Theory—The foundation of this theory is built on the premise that legitimacy is important to the successful operation of any entity (DiMaggio and Powell 1991) since it is in accordance with social rules and anticipations introduced by stakeholders. Massey (2001) explains that managing legitimacy is a customary procedure by which institutions try to obtain, maintain and recoup stakeholder backing for their actions. He adds that for legitimacy to be retained, institutions ought to be involved in successful management of crises. From the lens of neo-institutionalism, Coombs and Holladay (1996) argue that organizations must adopt crisis response strategies that demonstrate attempts to re-institute legitimacy. Institutions are advised to move their attention from contravening social norms to renovation of the breaches whilst demonstrating how they have reverted to their stakeholders' standards.

Attribution Theory—According to Coombs and Holladay (1996) this is a fundamental concept for elaborating the connection between the choices of communication strategies to a situation. Bernard Weiner, a specialist in this theory asserts that if an event's outcome is unpredictable, negative or essential, people will investigate their causes (Weiner et al. 1988) and once they find out the cause of the crisis, they place blame on the authority responsible. In essence, bigger ascription of responsibility gives rise to heightened sense of anger and an unfavorable perception of an entity's reputation (Weiner et al. 1987). Pertinently, the attribution theory professes that people assess causes of incidents depending on their controllability, stability and locus (Weiner 1986). Wilson et al. (1993) elaborate that controllability judges whether causes that lead to some incidents are influenced by an actor (controllable) or are beyond an actor (uncontrollable). Stability judges whether an incident's cause is ever existent (stable) or is seasonal and differs based on circumstances (unstable). Locus judges whether an incident's cause is within an actor (internal) or is within a situation (external).

Consequently, Russell (1982) developed Causal Dimension Scale—a mechanism designed to evaluate how people discern causes for events—which helps to create two dimensions of crises matrix: internal-external and intentional unintentional. While internal-external dimension describe either self-inflicted or unconscious actions from an entity, intentional-unintentional dimension points to how controllable certain events are. Coombs (1995) employs these dimensions to come up with four types of crises: faux pas and accidents which are grouped as unintentional crises; and transgressions and terrorism which are conceived as intentional crises. He goes on to assert that the publics ascribe blame on an institution based on the evidence that there is actually a crisis, the damage that a crisis causes and the history of an entity in preventing or dealing with previous crises (Coombs 1995: 454–469).

6 Methodology

Qualitative interviewing was chosen as the technique to address the Research Questions. Participants for the study, especially journalists, security experts, digital PR experts and Communication Authority of Kenya officials were selected based on their scholarly and years of professional experience.

Research Questions

The following research questions are explored:

RQ1. How are SNS users accountable in the global war on terrorism?
RQ2. How important are SNS in furthering the interests and agenda of terrorists?
RQ3. How effectively do governments use SNS in risk and crisis communication with regards to terrorism?

7 Research Findings and Results

7.1 RQ1: How Are SNS Users Accountable in the Global War on Terrorism?

This question was asked to all participants except security experts as their responses were solely confined to security related issues regarding social media. To answer this question, participants were asked how they make meaning of accountability with regards to terrorism in the age of social media. All participants agreed that accountability meant responsibility, but differed on whom to be accountable to. While discussing responsibility, three themes emerged from it; responsibility to self, responsibility to the audience and responsibility to the employer. Bloggers and members of the public who use social media felt that they are only accountable to themselves, while journalists, digital PR experts and government officials were unanimous that they are accountable to themselves, their audiences and their employers.

7.2 Responsibility to Self

Bloggers and members of the public defended their stand on why they felt they did not need to be answerable to anyone. One participant was very categorical and said:

> Social media was created so that any individual around the world could express themselves without being answerable to anybody. If we are to be answerable to another authority, how else would it be different to mainstream media?

On whether it is responsible to retweet or share on Facebook an incident of a terror attack or an unverified statement from a terrorist account regarding an attack, a participant responded:

> Yes. In the past, we used to rely on mainstream media or the government to release a statement about such an attack but social media is the most important revolution ever. Now I feel like I have a voice. I can tweet at the Inspector General of police, cabinet secretary of internal security and even the president. This is one of the ways to make them act on things that would have otherwise gone unnoticed or taken long.

Another participant concurred:

> Speech should be countered by speech. If I have posted something offensive, then I leave it to my audience to judge me. Even then, I would still consider their criticism as 'their opinion' which won't dissuade me from relaying what I feel.

One of the participants had a different opinion from her colleagues;

> I have been blogging and using Twitter and Facebook for so many years. I know the pros and cons of content. Just because social media is unregulated does not give us the freedom to post things without much thought. We cannot compromise the security of the society we live in knowingly by giving terrorists too much of a voice.

Digital PR experts however felt that social media should not be treated differently from other communication tools, emphasizing that responsible micro-blogging is necessary for the good of the society especially when it comes to terrorism issues. One of the digital content participants said:

> Given that social media are used by people of varying age, exposure and other variables, it is expected that some users don't have the sense to be more responsible in their postings and as such they post things that are considered offensive by other people. The question is; how do you make them accountable? There's no law that deals with that holistically. The only way is probably to spend time educating the public on the responsible use and the effects it has on countering terrorism.

Communication Authority of Kenya officials were also keen to see social media users demonstrating more caution and becoming accountable to themselves. One participant described some of the online behavior as "attention-seeking" in order to gain more followers at the expense of people's emotions:

> To be honest, I have seen excesses and recklessness on social media that borders on glorifying terrorists. Some people resort to sensationalism and dangerous rumour-peddling which can easily lead to anarchy. Being ethical and sensitive to security issues can go a long way in winning the war on terror.

In explaining how accountable they are to themselves, most journalists recounted past terror attacks in Kenya and how they impacted their personal emotions. For instance, one of the participants said:

> "We are first human beings then journalists and the bit about being human is that we have emotions. I reported the Westgate terror attack of 2013 from the frontline as well as the Garissa University College massacre in 2015 and I felt like I was part of the victims". This reporter added that he would not tweet or share information that gives terrorists a psychological boost during a crisis.

Most reporters cited examples of how the numerous terror attacks in Kenya have influenced their social media interaction and reporting. One of them said:

> During the Westgate attack, I thought that by revealing a lot of information on what the security apparatus was doing to contain a terrorism crisis, I was doing a wonderful job as a journalist but I later realised that my information could be used by terrorists to their advantage and cause more damage or make the situation worse.

7.3 Responsibility to the Audience

The Westgate attack was a watershed moment in how reporters and mainstream media in general engaged the audience on social media. In fact, it's after the Westgate attack that major media establishments took on the idea of training their journalists on the use of social media in the midst of a terror attack. All of them were unanimous that they had to report what would be considered sensitive to the audience. One participant gave reasons as to why such cautious steps are necessary in the age of social media:

> As much as we value objective reporting and the fact that members of the public deserve to know the truth about what is going on, we came to the agreement that we have a responsibility of ensuring we don't stimulate fear-mongering. Can you imagine the consequences of tweeting or sharing alarming messages and gory pictures of victims on social media yet one of the people who follow your account on Twitter have a family member who works or resides at the scene of the attack?

On the other hand, bloggers and ordinary users of social media were divided on the issue of whether the public deserved to know every detail at the expense of security and other sensitive issues during a terror attack. Some of them supported their stand on the basis that a democratic country should not be secretive about anything, while others were downright opposed to indiscriminate sharing of information. One of the participants who supported relaying of information they stumble upon indiscriminately claimed:

> "We are in the age of information where social media has bestowed power and freedom to the common man. If we don't give a clear picture of what has happened, the public may fall for masked stories and endanger themselves because of that very lack of information. In a nutshell, we are helping to make our unresponsive government to act in a timely manner". He further claimed that his follower ratings on his social media account are proof that he is

> a trusted source. "Currently, I have over 70,000 followers. The fact that I gained a lot of followers, from my tweets and Facebook posts during the terrorist attack at Westgate is an indicator that I was judged to be a credible source", he added.

A blogger who did not agree with her colleague said:

> Although I'm in the business of informing the public, I have to exercise restraint in some of the things that my audience consumes. I always put myself in the shoes of the victims. So ask yourself, by posting too much detail, am I endangering the victims? Am I hurting the relatives? Will it worsen the current security crisis? All these questions can help inform a wise decision.

Digital PR experts gave their view based on their experience before the emergence of social media and compared it to present times. According to them, all forms of communication are targeted towards a certain audience, including the ones relayed by terrorists and therefore must be clearly thought through. One of the seasoned PR participants said:

> Let's assume I am a terrorist and I have social media accounts on Facebook, Twitter etc.; its only natural that I would like to get my message across to everyone and hope that it has a great impact. As a PR professional trying to counter their message, I would want their message to have very little penetration and impact. This shows how accountable we should be to the audience and it is a timeless rule.

One of her colleagues added:

> If I read my timeline on social media, I see the users divided into those who know the consequences of such indiscriminate posts and those who are ignorant. Everyone can blog or micro-blog, but there those who know what they are doing and there are those who don't. Some of them believe that if a post is on their timeline, they need to share, which is a very wrong habit.

While acknowledging that opportunities for self expression has grown exponentially in the age of social media, Communication authority officials bemoaned insensitive content that can spread panic and other negative effects. One of the participants said that it was imperative for online content to be given a lot of thought before being posted in the public.

> It does not make any sense for social media users to attempt to score a few cheap points at the expense of a crisis. It is out rightly distasteful if not warped.

7.4 Responsibility to Employer(s)

The concept of being answerable to employers did not impact on all participants but was pertinent to journalists and digital PR experts. Several journalists claimed that they took into account the policies of their media establishments when commenting on different issues on social media as some of them have been admonished in the past owing to their heedless posts. A few of them said that some online debates are so exciting and they sometimes get tempted to defy their employers' policies but were clever enough to protect themselves by putting disclaimers in their account profiles. One journalist said:

> Once in a while you find that you are tagged in some intense exchanges and you simply can't let it pass. Luckily for a lot of us, there is usually that magic phrase 'opinions expressed here are personal and do not reflect that of my employer'. In the absence of this disclaimer, it would be difficult to keep our jobs.

Digital PR experts on the other hand were so emphatic that they would always be respectful of their employers' needs in every single way. One of them said she knows of a colleague who made a silly mistake on her that cost him his job.

> For us in this industry, we tend to get hired by so many institutions within the same circle, so one little faux pas can be seen as a mortal sin and greatly reduce your chances of ever associating with any brand.

Overall, RQ1 findings indicated that social media responsibility to various entities mattered less to bloggers and ordinary users of social media but was a major factor to regulators of communication, journalists and digital PR experts who identified with particular institutions and establishments.

Another fundamental point that has come to light is that bloggers and ordinary users of social media show varying understanding of how their social media content can affect security operations during a terrorist attack. While young users (especially 25 years and below) feel that they can post anything and everything that comes to their attention, the older users (mostly aged 30 and above) see the need to exercise caution in whatever they post on their timelines.

The third conclusion is that there seems to be some 'herd mentality' influencing social media cumulative behavior, especially with regards to young users of social media, who see their ratings go higher as a result of posting frequently during a crisis, regardless of whether their information is verified or unverified.

RQ2: How important are SNS in furthering the interests and agenda of terrorists?

Under this research question, the social network platforms that were examined were Facebook, Twitter and Whatsapp. In general, participants were unanimous that Facebook was a powerful tool for terrorists owing to its overwhelming popularity amongst all other social media platforms.

Security experts and digital PR experts examined Facebook in terms of its features such as 'Like' and 'share' buttons which are mostly used by terrorists to spread their message among their sympathizers and supporters. They also claimed that the ability to form a community, network or a closed group meant that terrorists would be able to come together without necessarily meeting physically.

For instance one of the security experts said:

> With various features such as these, along with the inbox, messenger and even the timeline, Facebook gives terrorists a lot of room to communicate and share their jihad messages throughout the world. We have already seen militant groups like TTP advertising jobs for people to be recruited on a timeline that is public, what should worry most counter-terrorists is their brazen nature to go after vulnerable people.

Another security expert said there was a danger in many young people getting radicalized through Facebook:

> If this is the most popular social networking site in the world with more than a billion subscribers, you can imagine the thousands of young people who fall prey to religious propaganda in a naïve manner.

This discussion about features was prevalent among all participants who believe that they aid terrorism in a big way because they offer limitless space for most of their intentions, namely: radicalization, recruitment and propaganda.

In relation to Twitter, all participants seemed to believe that terrorists use this medium particularly for propaganda and radicalisation and a lot less for recruitment. One participant gave reasons as to why it met the terrorists' purpose of propaganda:

> The fact that Twitter limits characters to 140 characters makes it ideal for propaganda because the tweets posted will highly likely be short and precise in terms of glorifying their goals or despising the treatment received from what they call 'infidels'. One only needs to read the message being passed on and they tend to gain followers just by being retweeted by those who endorse such messages.

Most participants believed the retweet feature on Twitter is the most influential thing which makes it so popular. Another participant said:

> You don't need to be a regular tweeter or have many followers to make the terrorists messages reach a wider audience. In fact, one can just be an inactive user but the fact that a message is retweeted severally by a large number of users it meets its objective. The second thing that has become fashionable among Twitter users is the use of hashtags which makes a topic 'trend' or become a popular topic of discussion and therefore gain the attention it is meant to attract.

Participants were also in agreement that in light of limited space on Twitter, most terrorists use images on their twitter timelines to punch their point home. For example one participant said:

> As we know a picture is worth a thousand words, and since Twitter limits the number of characters to 140, one image is enough to pass a message. Terrorists have become witty and turned this disadvantage into an advantage because they post gory pictures of those they have murdered so that they are seen as heroic acts and try to encourage others to stand up for their doctrine.

To investigate WhatsApp more comprehensively as a medium, all participants were first asked whether they preferred using their mobile service provider text messaging or whether they preferred web-based instant messaging like WhatsApp. Overwhelmingly, all participants said they prefer using WhatsApp because they believed it gave them more privacy compared to mobile service providers.

Many participants believed WhatsApp was used by terrorists as a tool used for covert operations. One security expert said:

> WhatsApp makes communication very discrete and therefore gives terrorists a field day in carrying out their operations. All they need is an internet connection and they can plan the most atrocious things ever. Currently, WhatsApp has improved its features and instead of

> accepting people in groups of 50 like it was previously, it now takes up to 100 people of common interest. With these numbers, their logistics are made much easier as they are communicating 'from one room'. If for instance terrorists attacked a certain place and they have access to the internet, they would communicate seamlessly unhindered, using WhatsApp as their 'command and control centre'. This is what should worry many counter terrorist experts.

The medium seemed to attract a lot of discussion as it was claimed that it is also used for recruiting vulnerable people into terrorist activities. One participant (a student from one of the main universities) said:

> Sometime at the end of last year, I received a WhatsApp message from an unknown number on my phone asking me to set aside time for a very important meeting. On inquiring who it was, the sender just told me it's a 'friend' who wanted me to help save *Allah*'*s* followers. I asked him where the person got my number and he told me that it was given by a 'trusted' friend of mine. I engaged the person in the conversation for about two hours only to realize that he wanted me to join Al-Shabaab. He even enticed me with a lot of money some of which he said would be given to my family in advance as a form of appreciation.

He said that he resisted the advances but thought that if he reported the matter to authorities he did not trust the authorities to protect him:

> All the while I was terrified at these advances and I kept deleting the messages he sent me just in case someone snooped on my phone. After the third approach, I emphatically told him to keep off and I even blocked his number. For me, the WhatsApp feature that blocks another number is my favourite.

Overall, under RQ2, participants were unanimous in agreement that SNS and platforms play a far greater role in furthering the agenda of terrorists in terms of planning and recruitment. This was attributed to their popularity especially among younger generation and the unrestricted features that provide discrete communications.

RQ3: *How effectively do governments use SNS in risk and crisis communication with regards to terrorism?*

To address this question, participants were first asked to explain what they understood by risk communication and crisis communication. The most common theme expressed by the participants was the negative undertones associated with risk and crisis. One participant noted,

> Risk communication is about relaying information to the public about the dangers of something while crisis communication involves transmitting information that is meant to ease a critical situation or event that has occurred.

Most of the participants described risk as a "potential crisis" while describing crisis as a "potential disaster". Nonetheless, all of them were in agreement that sometimes terrorism-related risks and crises are sometimes unforeseen. All the participants also talked about the reputation of the government being at stake as a result of terrorism-related risks and crises.

Participants across the board took the stand that governments were not proactive when it came to risk communication regarding terrorism. They all agreed that governments were reactive. One participant said:

> Most governments have been very lackadaisical in communicating terrorism risks to the public. Most governments spend their time on crisis communication than risk communication. What you see most of the time is damage control. Here in Kenya, even after the Westgate attack, I didn't see any campaigns educating the public. It's only after the Garissa University attacks that the government started communicating. Even then, their risk communication has mostly been confined to mainstream media and very little on social media.

This observation was echoed by another participant:

> If terrorists are getting their messages across on social media with a lot of impact, why does the government eschew these channels and still resorts to traditional media? We have a dedicated digital communications department in the presidential strategic communications unit but you will see very little of educating people.

Another participant added:

> It is counter-productive for governments to use traditional media in trying to communicate the threat of terrorism. If we all agree that most young people are radicalized and recruited through social networks then it follows that governments should use the same channels to reach out to them and try to de-radicalise them. It is a no brainer!

One participant disagreed with the notion of regularly trying to communicate terrorism risks. He argued that the more the issue of terrorism is made a frequent subject, the more some young people may find it interesting through curiosity while others may get affected negatively as a result of their ordeals:

> When it comes to terrorism, I don't think you need to keep reminding the public about what to do or how to handle it. The question here should be examined based on the regularity. How many times should it be done? This is not easy because filling the news with a lot of terrorism warnings as it is an issue that creates an atmosphere of fear and for those who have experienced it first hand, it just prolongs trauma.

On crisis communication, many participants said that governments' crisis response strategies are mostly poorly established but tend to improve only after a major crisis occurs. They felt that without being tested, governments get complacent about putting any crisis communication plans in place. For instance, one participant said:

> Before the Westgate mall attack, the government had no social media crisis response strategies in place and that was evident as the siege was unfolding. We saw a lot of cluttered communication from numerous government officials. There was no clear spokesperson during that critical time until the second of the siege. The conflicting communication coming from the cabinet secretary for Internal Security, the Foreign Affairs cabinet secretary and the Chief of Defense Forces made them look like amateurs and resulted in the loss of faith and credibility by Kenyans on Social Media. Nobody knew who to trust or whose word to take.

Participants also said that many government officials were rookies when it came to using SNS and that was mostly an observation based on their message packaging during a crisis. One participant referred to a tweet by Inspector General of police during the Westgate mall attack that sounded so casual and in bad taste especially towards the affected families. A digital PR participant remarked:

> Everything seemed to have picked up well after day one until the Inspector General tweeted 'We're not here to feed the attackers with pastries but to finish and punish them'. Those of us in the PR world could not believe that someone who was being looked up to by Kenyans to provide information that imparts confidence could come up with such a blooper. He may have meant well but the way it was formulated attracted a deluge of criticism. Many people thought that the terrorism incident was a serious issue but it was being treated in a nonchalant way. Utterly shocking!

All participants claimed that the worst failure by governments is to keep the public away from their crisis management plans. In reference to Westgate mall attack, they said the government could not successfully rebuff Al-Shabaab's claims. They added that the while Al-Shabaab had one Twitter account that live-tweeted the siege, the government had many accounts that provided conflicting information. Participants said that the government would have 'crowd sourced'—soliciting contributions from the public SNS users or the online community—public support to counter Al-Shabaab's Twitter content. One participant said:

> In such situations the government wants to be seen that they are in charge and will sort out everything on their own but they forget that in the world of social network sites, you need a network of well wishers and good-will ambassadors to help you do the job. If terrorists are using one twitter account to spread their propaganda and the government uses multiple conflicting accounts, people will naturally believe the terrorist's account that stays on the message than the government. It's as simple as that.

Another participant added:

> Governments may be worried about protecting their reputation and relinquishing their duties and control in transmission of information, but they forget that times have changed and the methods of information gathering and distribution have changed too. Social network sites provide a great opportunity for governments not only to relay urgent and critical information during a crisis, but also to crowd-source situational information from afflicted people on the scene.

Most participants said that they saw a noticeable improvement after the Westgate mall attack. They claimed that great lessons were learnt and applied during the Garissa University College terror attack. A participant remarked:

> The crisis communication was an absolute improvement post-Westgate which actually demonstrates that governments improve their strategies after critical events.

In conclusion, RQ3 suggests that governments have not been very effective in their use of SNS vis-à-vis terrorism risk and crisis communication. Evidence has been indicated that most governments are slow in embracing SNS especially because they have not been tested by major crisis. It has also been demonstrated that SNS accounts are exemplified as 'spokespeople' and therefore many government accounts reporting on a crisis with varied information can lead to loss of credibility by the public. The third finding is that some government officials are poor at message packaging during a crisis and that sends very poor signals to the public. The fourth finding is that in the age of SNS where anyone with a cell phone can report anything, governments need to embrace the public or online communities as one way of achieving and countering terrorists' propaganda messages.

8 Discussion

This research explored how SNS are used by terrorists, public and governments in the atmosphere of risks and crises. It examined the participants' use of SNS and their accountability, the importance of SNS to terrorists and the efficiency with which governments use SNS in communicating terrorism risks and crises. The research has established a better understanding of the connection of SNS to terrorism, governments, publics, risks, crises, and communication.

Overall, participants interviewed for this research unanimously agreed that SNS have greatly influenced how risks and crises are managed and responded to in relation to terrorism. It is evident that terrorists have become more aggressive and adroit at using new communication technologies. Consequently, risk and crisis communication are now at the core of SNS determined by diverse variables: misleading information spreads faster and widely than it was previously; audiences are multifaceted as a result of being both consumers and content creators; anonymity online has eroded trust and thus creating high demand for *bona fide* sources; finally, decision on whether to communicate risks or respond to crises is made expeditiously.

It was also revealed that participants had different understanding of freedom of expression with regards to SNS, with some believing that regardless of potential risks or crisis, they felt no need for exercising restraint or caution. To them, SNS grants them outright freedom that should not be called into question. On the other hand security experts interviewed revealed that countering terrorism propaganda and covert communication will remain a challenge for as long as custodians of SNS do not actively pursue policies that will censor known terrorists.

It has also been noted that governments respond better in risk and crisis communication with every incident because the first incident somehow serves as some sort of "organizational learning". For instance, the terrorism incident on Westgate mall was seen by many analysts as a failure by the Kenyan government in risk and crisis communication messages but also as a learning opportunity. These lessons were demonstrated during the Garissa College University terrorist attack where they showed their improvement in coordination and having a single spokesman for all the updates regarding the attack.

A paramount observation from this study indicates that amongst all SNS, Twitter has been seen as the most popular and widely used both by governments and terrorists in communication. This can be attributed either to the ease of recipients understanding the information relayed owing to the limited character requirements or the fact that the retweet feature helps to make messages go viral faster than the rest.

Efficient risk and crisis communication is paramount for maintaining government—public relations as well as gaining or restoring credibility. From the interviews, sections of the public can be resourceful if their support is tapped during a crisis, while other members of the public can make crisis management a challenge by their actions.

Institutions need to come up with procedures that shield them from public indictment. As conceived by Shari et al. (2011) this research provides an overview of best practices in risk and crisis communication as follows:

- Set up risk and crisis management strategies which should involve standard procedures targeting pre-crisis (including risk communication), crisis and post crisis phases. The strategies should include practices such as civic education to the public.
- Design pre-event plans which should comprise identification of requisite resources, potential hazards, harmonisation of both internal and external communication processes and designation of responsibilities for staff.
- Collaborate with the public by sharing available information on time and accurately, as well as demonstrating readiness to receive essential information from the public.
- Pay attention to the populace and understand their fears. This should be done through dialogue, with or without evidence of risk, and gauging public opinion regarding risk.
- Relay information in an honest and transparent way before and after a crisis to dissuade the public from turning to other sources of information.
- Partner with reliable sources to ensure consistently credible and accurate information that portrays the institution to be trustworthy.
- Fulfill the media's demands by being reachable, as the public obtains risk and crisis information from them.
- Establish a sense of credibility with the public through honest regard of the plight. This would make the public reciprocal in terms of support and compassion.
- Be hesitant and accede to ambiguity as part of the strategy to re-organise and package information in the most appropriate manner. A hastily relayed inaccurate information or message from an institution—for the sake of timely response—is always difficult to be rebuffed by the same institution, leading to loss of faith by the public.
- Grant stakeholders permission to attain the perception of supervision, which helps to impart a feeling of resourcefulness amongst them.

9 Conclusion

Presently, a lot of research is confirming the great potential of SNS in risk and crisis communication but some governments have not embraced them as much as they should. Consequently, those that have adopted them have not been able to employ them critically in order to deliver information comprehensively to their target audience. The findings of this research indicate that social media have become a threat when used by terrorists because of certain privacy features they possess such as anonymity and end-to-end encryption. The onus is on companies that own these

SNS companies to be as innovative in creating solutions as they were in creating these platforms.

Secondly, some sections of the general public are not educated or informed on the moral duty of not furthering terrorists' agenda by sharing content in a way that affects and jeopardises security operations during an attack. Thirdly, owing to the fact that user policies of SNS are not unanimous and have not been streamlined to reflect their seriousness in policing online content, terrorists have taken advantage of this status and as such, security experts see these companies as a hindrance to Global war on terror. The few times they have cracked down on the terrorists online activities indicate that if they dedicate sufficient resources on coming up with technology that suppresses their activities or dedicate unwavering commitment to online policing then a significant step will be made towards solving the problem.

On issues of legislation, governments must come up with policies requiring SNS companies to constantly monitor users' content especially during a terror attack and cooperate with them in terms of turning in existing evidence on demand. While this may not be a panacea to the general problem related to all terrorism-related SNS issues, governments (such as the US) in which the SNS companies are located must lead the way in establishing trust with these companies as one of the many approaches of dealing with the matter.

Future research should move to the next phase where features of social media are examined in terms of how they can be transformed to become collaboratively useful for security experts, intelligence services and custodians of the same platforms in managing security risks and crises.

References

Al Jazeera (2013a) Al-Shabaab in long-running battle with Twitter. Available online at: http://www.aljazeera.com/indepth/features/2013/12/Al-Shabaab-long-running-battle-with-twitter-2013121711271555968.html. Accessed 5 July 2015

Al Jazeera (2013b) Kenyans tell minister: Westgate facts don't add up. Available online at: http://stream.aljazeera.com/story/201309302016-0023074. Accessed June 30 2015

Beck U (1992) Risk society: towards a new modernity. SAGE Publications, London

Berger JM (2013a) Terrorists on social media: arguments that don't impress me, Intel wire. Availale online at: http://news.intelwire.com/2013/10/terrorists-on-social-media-arguments.html. Accessed 8 June 2015

Berger JM (2013b) Twitter's week of reckoning. Foreign Policy. Available online at: http://www.foreignpolicy.com/articles/2013/10/01/twitters_week_of_reckoning#sthash.aObyjqaY.dpbs. Accessed 8 June 2015

Berube DM, Faber B, Scheufele DA, Cummings CL, Gardner GE, Martin KN, Martin MS, Temple NM (2010) Communicating risk in the 21st century: the case of nanotechnology. Available online at: http://www.nano.gov/sites/default/files/pub_resource/berube_risk_white_paper_feb_2010.pdf. Accessed 10 Aug 2015

Borodzicz EP (1996) Security and risk: a theoretical approach to managing loss prevention. Int J Risk Secur Crime Prev 1(2):131–143

Borodzicz EP (2005) Risk, crisis and security management. Wiley, West Sussex

Bronskill J (2001) CSIS on alert for cyber saboteurs: spy agency monitors threat to computer networks: report. Ottawa Citizen

Business Daily (2015) Facebook eyes Kenya office after South Africa. Available online at: http://www.businessdailyafrica.com/Corporate-News/Facebook-eyes-Kenya-office-after-South-Africa-entry/-/539550/2770834/-/item/0/-/n8m28wz/-/index.html. Accessed 18 July 2015

Business Insider (2015) The FBI claims technology promoted by Apple and WhatsApp is helping ISIS. Available online at: http://uk.businessinsider.com/fbi-encryption-going-dark-isis-apple-facebook-whatsapp-steinbach-lieu-2015-6. Accessed 2 Aug 2015

CNN (2013) How terror can breed through social media. Available online at: http://edition.cnn.com/2013/04/27/world/rivers-social-media-terror/. Accessed 5 July 2015

Communications Authority of Kenya (2015) Quarterly sector statistics report: third quarter of the financial year 2014/15. Available online at: http://www.ca.go.ke/images/downloads/STATISTICS/%20Sector%20Statistics%20Q3%202014-2015.pdf. Accessed 4 Aug 2015

Coombs WT (1995) Choosing the right words: the development of guidelines for the selection of the "appropriate" crisis-response strategies. Manage Commun Quarter 8:447–476

Coombs WT (1999) Ongoing crisis communication: planning, managing, and responding. Sage, Los Angeles

Coombs WT (2000) Crisis management: advantages of a relational perspective. In: Ledingham JA, Bruning SD (red). Public relations as relationship management

Coombs WT (2007) Protecting organization reputations during a crisis: the development and application of situational crisis communication theory. Corp Reputation Rev 10(3):163–176

Coombs WT, Holladay SJ (1996) Communication and attributions in a crisis: an experimental study of crisis communication. J Publ Relat Res 8:279–295

Daily Mail (2015) Fanatics are using secret message apps says anti-terror Tsar: government set to do battle with web giants including WhatsApp and Facebook after warning in landmark report. Available online at: http://www.dailymail.co.uk/news/article-3119167/Fanatics-using-secret-message-apps-says-anti-terror-tsar-Government-set-battle-web-giants-including-WhatsApp-Facebook-warning-landmark-report.html. Accessed 2 Aug 2015

Denning D (2000) Cyber terrorism special oversight panel on terrorism committee on armed services, U.S. House of representatives May 23, 2000. Available online at: http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf. Accessed 3 June 2015

Denning D (2010) Terror's web: how the internet is transforming terrorism. In: Yar M, Jewkes Y Handbook of internet crime. Willan Publishers, London, pp 194–212

Dewing M (2012) Social media: an introduction, Publication No. 2010-03-E. http://www.parl.gc.ca/content/lop/researchpublications/2010-03-e.pdf. Accessed 5 June 2015

DiMaggio PJ, Powell WW (1991) Introduction. In: DiMaggio PJ, Powell W (eds) The new institutionalism and organizational analysis. University of Chicago Press, Chicago. pp 1–38

Entman MR (2004) Projections of power: framing news, public opinion, and U.S. foreign policy. University of Chicago Press, Chicago

Facebook (undated) Community Standards. Available online at: https://www.facebook.com/communitystandards. Accessed 3 July 2015

Fischhoff B (2002) Assessing and communicating the risks of terrorism. In: Teich A, Nelson S, Lita S, Hunt A (eds) Science and technology in a vulnerable world. DC, AAAS, Washington

Fischhoff B (2006) Psychological perception of risk. In: Kamien D (ed) The McGraw-Hill homeland security handbook. McGraw Hill, New York, pp 463–492

Fox RL, Gangl A (2011) "News You Can't Use": politics and democracy in the new media environment. In: Le Cheminant W, Parrish JM (eds) Manipulating democracy—democratic theory, political psychology, and mass media. Routledge

Freberg K, Palenchar MJ (2013) Convergence of digital negotiation and risk challenges. In: Social media and strategic communications. pp 83–100, Palgrave Macmillan, UK

Gertz B (2013) Islamist Terrorists shifting from web to social media. The Washington Free Beacon. Available online at: http://freebeacon.com/islamist-terrorists-shifting-from-web-to-social-media/. Accessed 21 July 2015

GlobalWebIndex (2013) Twitter now the fastest growing social platform in the world. Available online at: http://blog.globalwebindex.net/twitter-now-the-fastest-growing-social-platform-in-the-world/. Accessed 10 July 2015

Gray GM, Ropeik DP (2002) Dealing with the dangers of fear: the role of risk communication. Health Aff 21(6):106–116

Guardian (2014) WhatsApp adds end-to-end encryption using TextSecure. Available online at: http://www.theguardian.com/technology/2014/nov/19/whatsapp-messaging-encryption-android-ios. Accessed 2 Aug 2015

Irwin A (1995) Citizen science: a study of people, expertise and sustainable development. Routledge, London

Kasperson RE, Kasperson JX (1996) The social amplification and attenuation of risk. In: Hunreuther H, Slovic P (eds) Challenges in risk assessment and risk management. The Annals of the American Academy, vol 545, no 1, pp 95–105

Kasperson RE, Palmlund I (2005) Evaluating risk communication. In: Kasperson JX, Kasperson RE (eds) The social contours of risk, vol 1., Publics, risk communication and the social amplification of risk earth scan, London, pp 51–67

Kohlmann E (2010) Hacking Al-Qaida: social networking, technology and terrorism. International Conference on Cyber Security (ICCS). Available online at: http://www.fordham.edu/Campus_Resources/eNewsroom/topstories_1916.asp (undated) See also http://iccs.fordham.edu/program/iccs2010/. Accessed 14 July 2015

Ledingham JA, Stephen DB (1998) Relationship management in public relations: dimensions of an organization-public relationship. Publ Relat Rev 24(1):55–65

Ledingham JA (2006) Relationship management: a general theory of public relations. In: Botan CH, Hazleton V (eds) Public relations theory II

Los Angeles Times (2013a) Twitter suspends account run by Al-Qaeda-linked Somali militants. Available online at: http://articles.latimes.com/2013/jan/25/world/la-fg-wn-twitter-suspends-shabab-20130125. Accessed 5 July 2015

Los Angeles Times (2013b) Kenya mall attack: official accounts of siege differ. Los Angeles Times. Available online at: http://www.latimes.com/world/worldnow/la-fg-wn-kenya-mall-conflicting-reports-20130924,0,7905720.story#axzz2pSZ6HQnK. Accessed 5 July 2015

Mag PC (2015) Definition of Twitter. Available online at: http://www.pcmag.com/encyclopedia/term/57880/twitter. Accessed 16 June 2015

Massey JE (2001) Managing organizational legitimacy: communications strategies for organizations in crisis. J Bus Commun 38:153–183

Nahon K, Hemsley J (2013) Going viral. Polity Press Cambridge, Cambridge

National Research Council (1989) 'Improving Risk Communication', National research committee on risk perceptions and communication. National Academies Press, Washington

New Statesman (2013) The Twitter Jihadis: how terror groups have turned to social media, New Statesman. Available online at: http://www.newstatesman.com/2013/08/twitter-jihadis. Accessed 3 July 2015

New York Times (1985) Thatcher urges the press to help 'starve' terrorists. Available online at: http://www.nytimes.com/1985/07/16/world/thatcher-urges-the-press-to-help-starve-terrorists.html. Accessed 30 May 2015

New York Times (2007) Defense secretary urges more spending for U.S. diplomacy, The New York Times. Available online at: http://www.nytimes.com/2007/11/27/washington/27gates.html?pagewanted=print&_r=0. Accessed 14 July 2015

O'Reilly T (2007) What is Web 2.0?—design patterns and business models for the next generation of soft ware. Available online at: http://yil5.inet-tr.org.tr/akgul/tmp/SSRN-id1008839.pdf. Accessed 30 May 2015

Pearson CM, Mitroff I (1993) From crisis prone to crisis prepared: a framework for crisis management. Acad Manage Executive 7(1):49–59

Perl RF (1997) Terrorism, the media and the government: perspectives trends and options for policy makers. Available online at: http://digital.library.unt.edu/ark:/67531/metacrs419/m1/1/high_res_d/97-960f_1997Oct22.htm. Accessed 3 June 2015

Portland Communications (2012) How Africa Tweets. Available online at: http://www.portland-communications.com/wp-content/uploads/2013/05/Twitter_in_Africa_PPT.pdf. Accessed 3 Aug 2015

Radio Free Europe (2013) How social networks are dealing with terrorists. Available online at: http://www.rferl.org/content/twitter-facebook-terrorists/24906583.html. Accessed 3 July 2015

Rogers MB, Amlot R, Rubin GJ, Wessely S, Krieger K (2007) Mediating the social and psychological impacts of terrorist attacks: the role of risk perception and risk communication. Int Rev Psychiatry 19(3):279–288

Russell D (1982) The causal dimension scale: a measure of how Individuals perceive causes. J Pers Soc Psychol 42:1137–1145

Schultz F, Utz S, Göritz A (2011) Is the medium the message? Perceptions of and reactions to crisis communication via Twitter, blogs and traditional media. Publ Relat Rev 37:20–27

Shari RV, Tara B, Michael JP (2011) A work-in-process literature review: incorporating social media in risk and crisis communication. J Contingencies Crisis Manag 19(2):110–122

Simon T, Goldberg A, Aharonson-Daniel L, Leykin D, Adini B (2014) Twitter in the cross fire—the use of social media in the westgate mall terror attack in Kenya. Available online at: http://www.plosone.org/article/fetchObject.action?uri=info:doi/10.1371/journal.pone.0104136&representation=PDF. Accessed 2 Aug 2015

Sky News (2013) Kenya siege: gunmen “Running and Hiding”. Available online at: http://news.sky.com/story/1145375/kenya-siege-gunmen-running-and-hiding. Accessed 6 July 2015

Standard Digital (2015) Study: terrorist groups recruiting Kenyan youth through social media. Available online at: http://www.standardmedia.co.ke/article/2000168474/study-terrorist-groups-recruiting-kenyan-youth-through-social-media?articleID=2000168474&story_title=study-terrorist-groups-recruiting-kenyan-youth-through-social-media&pageNo=1. Accessed 10 July 2015

Stewart DR, Coleman CA (2013) Legal and ethical use of social media for strategic communicators. In: Nor-Aldeen H, Hendricks JA (eds) Social media and strategic communication. Palgrave Macmillan, New York, pp 180–198

Strecher VJ, Greenwood T, Wang C, Dumont D (1999) Interactive multimedia and risk communication. J National Cancer Inst Monogr 25(134–139):135

Telegraph (2013) Twitter in numbers. Available online at: http://www.telegraph.co.uk/technology/twitter/9945505/Twitter-in-numbers.html. Accessed 10 July 2015

Wales C, Mythen G (2002) Risky discourses: the politics of GM foods. Environ Politics 11 (2):121–144

Weiner B (1986) An attributional theory of motivation and emotion. Springer, New York

Weiner B, Amirkan J, Folkes VS, Verette JA (1987) An attribution analysis of excuse giving: studies of a naïve theory of emotion. J Pers Soc Psychol 53:316–324

Weiner B, Perry RP, Magnusson J (1988) An attribution analysis of reactions to stigmas. J Pers Soc Psychol 55:738–748

WhatsApp (undated) How it works. Available online at: https://www.whatsapp.com/. Accessed 28 July 2015

Wilson SR, Cruz MG, Marshall LJ, Rao N (1993) An attributional analysis of compliance-gaining interactions. Commun Monogr 60:352–372

World Economic Forum (2013) Global risks 2013. Insight report. Available online at: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf. Accessed 22 July 2015

Wright DK, Hinson MD (2009) Examining how public relations practitioners actually are using social media. Publ Relat J 3(3):2–32

Manufactured Risk, Complexity and Non-traditional Security: From World Risk Society to a Networked Risk Model

Anthony J. Masys

Abstract Within the context of non-traditional security, this chapter reflects upon Beck's (1992, 2009) claim that we inhabit a Risk Society. With the advent of global climate change, extreme weather, transnational crime, NATECH's (natural disaster triggered technological disasters), and terrorism, Beck's notion of 'manufactured risks' resonates with the non-traditional security domain that includes: economic security, energy security, environmental security, health security and food security. This is all about complexity framing. Beck (1992) risk discourse regarding manufactured risks and effects that are both temporally and spatially displaced resonates with the complexity notion of nonlinearity. Hence the inherent interdependencies and interconnectivity that characterizes the risk space leads to a network model. The notion of hyper-risks (Helbing 2013; Masys et al. 2014) captures well the interconnectivity and complexity of the security threats. The complexity lens thereby becomes prominent in examining security. A networked risk model emerges as a construct that links Becks risk discourse to non-traditional security challenges.

Keywords Non-traditional security · Risk society · Terrorism · Human security · Networks

1 Introduction

Helbing (2013: 51) poignantly argues that 'Globalization and technological revolutions are changing our planet'. Along with the benefits and opportunities associated with worldwide collaboration networks comes 'pathways along which dangerous and damaging events can spread rapidly and globally'. With our hyper-connected world underpinned by hyper or hybrid-risks (Masys et al. 2014), the impact of unexpected events such as floods, earthquakes, financial crisis, pandemics and

A.J. Masys (✉)
University of Leicester, Leicester, UK
e-mail: anthony.masys@gmail.com

A.J. Masys (ed.), *Exploring the Security Landscape: Non-Traditional Security Challenges*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-27914-5_15

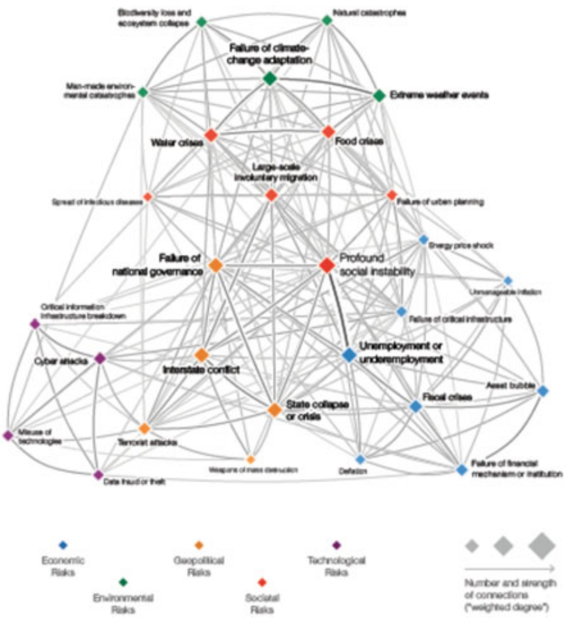

Biodiversity loss and ecosystem collapse
Natural catastrophes
Failure of climate-change adaptation
Man-made environmental catastrophes
Extreme weather events
Water crises
Food crises
Large-scale involuntary migration
Spread of infectious diseases
Failure of urban planning
Energy price shock
Failure of national governance
Profound social instability
Unmanageable inflation
Critical information infrastructure breakdown
Failure of critical infrastructure
Unemployment or underemployment
Cyber attacks
Interstate conflict
Asset bubble
Fiscal crises
State collapse or crisis
Misuse of technologies
Terrorist attacks
Weapons of mass destruction
Deflation
Failure of financial mechanism or institution
Data fraud or theft
Economic Risks
Geopolitical Risks
Technological Risks
Environmental Risks
Societal Risks
Number and strength of connections ("weighted degree")

Fig. 1 Global risks (WEF 2015)

cyber-attacks has revealed the fragility and vulnerabilities that lie within the social/technological/economic/political/ecological interdependent systems. Such events can have local, regional and global impact and thereby are a national security concern.

The WEF Global Risks (2015) illustrates the notion of hyper-connected risks highlighting to the security domain how risk has become transborder, interdependent and contagion rapid (Fig. 1).

The anticipation of catastrophe is changing the world. Events of 9/11, 7/7, Mumbia (2008), Spain (2004), extreme weather, SARS, pandemic risks (Ebola) and proliferation of ISIL and affiliates have become a central issue in shaping the risk and the security agenda. For example, the global reach of terrorism according to Mythen and Walklate (2008) remains a high consequence, low probability risk with the capability of generating irremediable effects. What emerges from the discourse regarding terrorism is the realization that '…national security is, in the borderless age of risks, no longer national security' (Beck 2002). Similarly, transborder health risks such as SARS and Ebola, can have significant impact on a nations economic and national security. Given this realization, research within the security domain is drawing upon Beck's analysis of risk society as a conceptual tool to make sense of and redefine the security agenda.

Helbing (2013: 51) argues that:

> Today's strongly connected, global networks have produced highly interdependent systems that we do not understand and cannot control well. These systems are vulnerable to failure at all scales, posing serious threats to society, even when external shocks are absent. As the

> complexity and interaction strengths in our networked world increase, man-made systems can become unstable, creating uncontrollable situations even when decision-makers are well-skilled, have all data and technology at their disposal, and do their best.

With this complex risk landscape, Beck's discourse on risk society provides a framework in which to understand non-traditional security. The risk society described by Beck (1992, 2009) maps well to the notion of network thinking (Masys et al. 2014; Masys 2015; Xu and Masys 2015) recognizing the interdependencies and interconnectivity that characterizes global risks.

2 Non-traditional Security

Today's security landscape has been described as transnational in nature. In light of this, the security studies domain has seen a deepening and broadening in response to the changing landscape. In addition to the issues pertaining to the traditional security concerns of threat, force and state actors, non-traditional security issues have emerged. The notion of human security described in the UNDP 1994 report identifies 7 themes that capture key elements that characterize some of the non-traditional security concerns:

- Economic security
- Food security
- Health security
- Environmental security
- Personal security
- Community security
- Political security.

These crosscutting and interdependent themes certainly challenge the traditional notions of security. For example, shocks to the global system stemming from natural disaster to man-made disasters comprise some if not all aspects of these themes in one way or another. Take for example the recent Ebola outbreak that had effects globally in shaping security and safety perceptions of risk. Borders were closed, migration curtailed, food security and health security challenged.

Similarly, diseases such as HIV/AIDS, malaria, TB-endemic in the low-income countries and emerging infectious diseases, such as SARS, avian flu (H5N1) and swine flu (H1N1) have been identified as threats to national and economic security because of the global interdependence and the disease characteristics that make them contagion rapid.

Transnational crime is becoming prominent in national security agendas. As described in the World Threat Assessment (2015: 8),

> Transnational Organized Crime (TOC) is a global, persistent threat to our communities at home and our interests abroad. Savvy, profit-driven criminal networks traffic in drugs, persons, wildlife, and weapons; corrode security and governance; undermine legitimate

> economic activity and the rule of law; cost economies important revenue; and undercut US development efforts.

The societal security effects of Drug trafficking emerges from increasing drug consumption and addiction, raising the level of violent crime, affecting health consumers, spreading HIV/AIDS and undermining family structures (Emmers 2013: 139).

With heightened awareness and concern regarding the proliferation and expansion of ISIL and connections to homegrown violent extremism, the complexity of the current threat landscape associated with terrorism continues to be a top national and global security agenda item (World Threat Assessment 2015: 8). Stemming from the violence perpetuated by ISIL, the securitization of undocumented migration has become a recurrent event. As described by the UNHCR (2015):

> By mid-2014, OCHA estimated that 10.8 million of Syria's 22 million population was affected by the conflict and in need of humanitarian assistance, including 6.5 million internally displaced, often multiple times - 50 per cent more than in 2013. If a comprehensive political solution is not reached, the number affected is expected to grow in 2015.
>
> Syria is hosting more than 33,000 asylum-seekers and refugees mainly from Iraq, with smaller numbers coming from Afghanistan and Somalia. In August 2014, approximately 95,000 people displaced by violence in Iraq entered the north-eastern Hassakeh governorate, although the majority proceeded onwards to the Kurdistan region to seek safety.

As described in Emmers (2013: 138), 'Migration is a complex social phenomenon that is influenced by economic, political, socio-cultural, historical and geographical factors'. This in itself contributes to the complex human security issue.

Environmental security has emerged as a significant security issue. Natural disaster and man-made disaster can have local and global effects. As described in Masys et al. (2014), recent disasters such as Hurricane Katrina (2005), Fukushima Daiichi nuclear accident (2011), Hurricane Sandy (2012), and Typhoon Haiyan (2013) highlight the vulnerability of communities to environmental and human-made disasters and the crippling effect that such disasters can have on the social and economic well-being of a nation. Contributing to the discourse on the link between environment and security, UN Secretary General Ban Ki Moon argues that, 'Climate change not only exacerbates threats to peace and security. It is a threat to international peace and security' (Barnett 2013: 193).

Energy security intersects and is interdependent with other security matters. From terrorism to natural disasters to NATECHs (Masys et al. 2014), all put strain on national and global security and can have '…significant consequences for international security, as inter-state cooperation threatens to break down into a struggle over the control of key energy reserves' (Raphael and Stokes 2013: 307). Raphael and Stokes (2013: 308) argues that '…the mismatch between the geographical distribution of world energy stocks and the location of the largest energy consumers creates what we will call an energy-security nexus, whereby energy security becomes irretrievably entwined with the wider foreign and security policies of key states'. The Fukushima Daiichi nuclear accident had global effects on reshaping the nuclear industry. The Washington Post (2015) reports:

> Only days after the nuclear meltdown in Fukushima, it became clear that the most long-lasting policy repercussions may not emerge in Japan, but far away in Europe. German Chancellor Angela Merkel, who had previously defended nuclear energy, rapidly reversed her stance and announced that Germany would gradually turn off all nuclear power plants forever. Nearly 60 % of Germans said in a 2011 survey that they considered it plausible that a similar disaster could occur in their own region.
>
> Eight of the country's 17 nuclear power plants were shut down within days after the Japanese catastrophe. Since then, the German government has worked on a long-term strategy to make it independent from nuclear energy as well as coal in the future.

The nontraditional security domain encapsulates the 'hyper risks' and hybrid risks (Helbing 2013; Masys et al. 2014) that characterizes the current threat and risk landscape that is shaping national and security agendas. As will be discussed in the following discourse, Beck's (1992) risk society theory also provides a crosscutting approach to understanding nontraditional security highlighting the notion of manufactured risks. This connects well to the networked risk model (Helbing 2013; WEF 2015; Masys et al. 2014; Masys 2015; Xu and Masys 2015).

3 Beck's Risk Society

The emergence of Beck's (1992) theory is framed along side a series of industrial disasters such as Bhopal (1984), Chernobyl (1986), Exxon Valdez (1989) and BP Deepwater Horizon Oil Rig disaster (2010) in which help to situate the argument within global, environmental, political, social and economic contexts. Emerging from this risk society thesis (Beck 1992) is the notion of manufactured risk—that draws upon a socio-technical discourse. Societal threats and vulnerabilities emerging from such vectors as Bovine Spongiform Encephalopathy (BSE), commonly known as mad-cow disease and Chlorofluorocarbons (CFC) represent manufactured risk that have significant security implications. The nature of risk and uncertainty have become overlapped, whereby risks have become more global '… more problematic, less easily manageable and more anxiety provoking' (Beck 1992).

Risk is not synonymous with catastrophe but rather has everything to do with the anticipation of the catastrophe. Risks therefore are concerned with the possibility of future occurrences and developments and thereby become present in a world that does not (yet) exist (Beck 2009). The anticipation of catastrophe shapes our expectations and mental models and thereby guides our sense making, decisions and actions. In this sense, risk can be seen to be a political force that transforms the world (Beck 2009).

The manufactured risks that characterize the risk society as described in Beck (1992, 2009), result in a preoccupation with debating, preventing and managing these very risks. Such risks move us from risk management to complexity management. Such examples as Chernobyl, mad cow disease, H1N1, CFCs and terrorism all reveal the trans-border and distributed nature of the risks emerging from the risk society, all resulting in unforeseen effects. Within this paradigm, risk is no longer localized but has become differentially distributed (borderless risk) thereby requiring society to deal with persistent insecurities and uncertainties. As such, risk aetiology and in particular the security agenda has become complex and reflexive and it requires a reconceptualization of the risk society perspective. What characterizes risk in the risk society according to Ekberg (2007: 344) is the shift in emphasis:

> …from natural to technological risks, the shift from a realist to social constructivist perspective on risk, the increasing gap between actual and perceived risk, the progression from invisible to visible to virtual risk and finally, the change in the spatial, temporal and demographic distribution of risk, giving rise to a new category of borderless risks. It is these salient features of risk in the risk society, rather than the presence of risk itself, that legitimate the claim that the risks of the risk society are exceptional.

The event of 9/11 reified that we now live in a 'risk society', a society in which there are uncontrollable and unpredictable dangers whereby terrorism emerges as a principal hallmark of the manufactured risk. Beck (2002) argues that the view of terrorism as a risk goes 'beyond rational calculation into the realm of unpredictable turbulence' thereby shaping the security agenda. As noted in Aradau and Van Munster (2007: 90), Rasmussen (2001) supports this notion recognizing 9/11 as a '…tragic example of a new asymmetrical strategic reality that is better understood by the concept of risk society than by traditional notions of terrorism'. These very characteristics of risk society have reshaped the notions of security and safety and thereby shape politics and public policy (Beck 2003). With the inherent uncertainty regarding the nature, medium and target, risk assessments become problematic and thereby require security agencies and governments to enact policies to address these manufactured risks characterized by uncertainty and reifying as anticipation (through management of risk: planning and preparation). The issue that permeates the risk society is '…how to *feign* control over the uncontrollable—in politics, law, science, technology, economy and everyday life' (Beck 2002). Global anticipation and expectation has influenced decision making and precipitated the emergence of resilience as the reaction to uncertainty. Beck (2009) argues that 'This means that the dynamic of risk society rests less on the assumption that now and in future we must live in a world of unprecedented dangers; rather we live in a world that has to make decisions concerning its future under the conditions of manufactured, self-inflicted insecurity'. Fukushima Daiichi (Masys et al. 2014) figures prominently.

As noted in Masys et al. (2014: 773) 'The 'networked' understanding of hyper-risks (Helbing 2013) requires a more holistic approach to hazard identification and risk management that transcends the linear agent-consequence analysis. With events such as the 2010 Ash Cloud stemming from the eruption of Eyjafjallajökull and the resulting disruptions to air travel and trade in Europe (Harris et al. 2012), we see how 'networked risks' are not confined to national borders or a single sector, and do not fit the monocausal model of risk'. As argued by Renn et al. (2011: 234) such risks or hyper-risks are '…complex (multi-causal) and surrounded by uncertainty and/or ambiguity'. It blends the ideas of manufactured risks and natural hazards such that challenges the linear Cartesian-Newtonian model of linear causality and replaces it with complex causality whereby time and space are folded (Masys 2010). The complex aetiology of such risks as disaster events described in Johnson (2008), Kroger and Zio (2011), Masys et al. (2014) and Masys (2015) requires the reconceptualization of risk society through a relational model.

These 'manufactured risks' are exemplified by nuclear power, chemical accidents and environmental pollution. It is from this that we can draw parallels and connections between Beck's risk society and complex networked risks. These networks are characterized by their physical, spatial and temporal heterogeneity. Because of the inherent complexity in these systems, they challenge our understanding pertaining to their structure and dynamics and thereby our understanding regarding vulnerabilities and their impact on society (Vespignani 2009: 425).

Vespignani (2010: 984) argues that because of the interdependencies of the CI such as those demonstrated by power generation grids, telecommunication, transportation, 'the failure or damage …would cause huge social disruption, probably out of all proportion to the actual physical damage'. What emerges is the realization that 'recent disasters ranging from hurricanes to large-scale power outages and terrorist attacks have shown that the most dangerous vulnerability is hiding in the many interdependencies across different infrastructures'. These interdependencies can be viewed in terms of the relationality inherent within the system and emerge from our 'manufactured world'. Such relationality has been described in Masys (2012a, 2012b, 2013), Wattie and Masys (2014) and Masys et al. (2014).

Analysis of vulnerabilities associated with hyper-risks requires the discipline of the systems approach which embraces a shift of mind: 'in seeing interrelationships rather than linear cause-effect chains and seeing processes of change rather than snapshots' (Senge 1990). Systems thinking thereby is an appropriate approach for communicating such complexities and interdependencies. The conceptual model suggests that there exists a disproportionality of 'causes and effects', in which as Urry (2002: 59) remarks, past events are never 'forgotten', they are seeded (manufactured) in the actor network (Masys 2012a, 2012b; Masys et al. 2014).

Risk society is ultimately a world risk society (Beck 2009) recognizing the delocalized nature of risk and its inherent spatial and temporal dimensions. This is noted in Masys (2014) in terms of socio-technical systems and misalignment where 'resident pathogens' become seeded or emerge within the complex networked aetiology (Fig. 2). The risks associated with the world risk society paradigm and the security agenda such as Ebola, climate change, and critical infrastructure prompt anticipation of global catastrophes and thereby destabilize the foundations of modern societies in terms of safety and security agendas.

As noted by Beck (2009), the inherent risks (resident pathogens) have a characteristic of delocalization such that cause and effect are non-linear (Fig. 2).

These characteristics shape the global safety and security agenda.

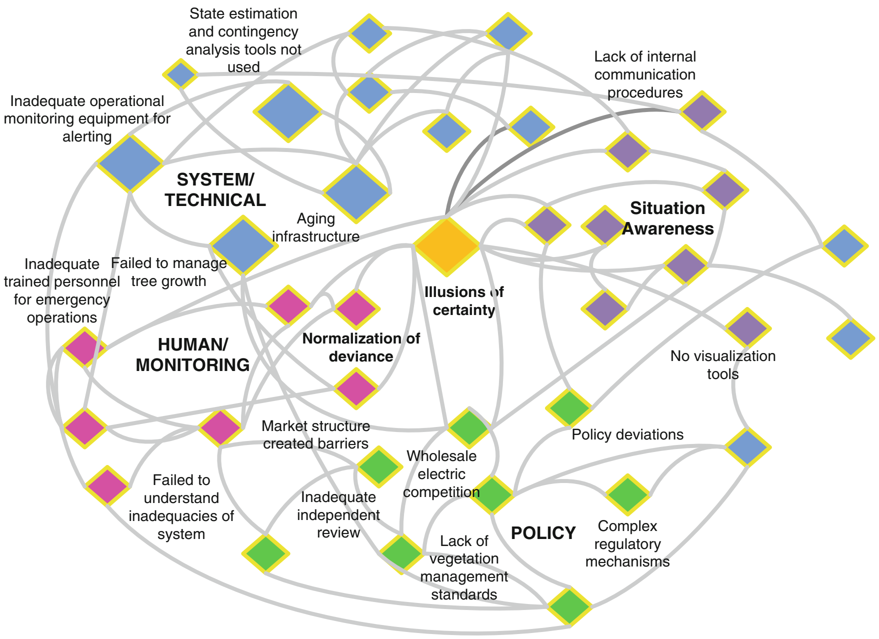

State estimation and contingency analysis tools not used
Inadequate operational monitoring equipment for alerting
Lack of internal communication procedures
SYSTEM/ TECHNICAL
Aging infrastructure
Situation Awareness
Inadequate trained personnel for emergency operations
Failed to manage tree growth
Illusions of certainty
HUMAN/ MONITORING
Normalization of deviance
No visualization tools
Market structure created barriers
Policy deviations
Wholesale electric competition
Failed to understand inadequacies of system
Inadequate independent review
POLICY
Complex regulatory mechanisms
Lack of vegetation management standards

Fig. 2 Actor network (resident pathogens) (Masys 2014)

3.1 Shaping the Security Agenda

In terms of this networked risk interpreted from Beck's risk society discourse, systems thinking figures prominently. Capra and Luisi (2014: 80–82) capture the key characteristics of systems thinking that resonate with the network model:

- Shift of perspective from the parts to the whole
  – Their essential or systemic properties are properties of the whole, which none of the parts have.
- Inherent multidisciplinarity
- From objects to relationships
  – In the systems view, we realize that the objects themselves are networks of relationships, embedded in larger networks.
- From measuring to mapping
  – Relationships cannot be measured and weighed; relationships need to be mapped.

- From quantities to qualities
  - The new mathematics of complexity is a mathematics of visual patterns, and the analysis of these patterns is known as qualitative analysis.
- From structures to processes
- From objective to epistemic
  - Isolating a pattern in a complex network by drawing a boundary around it and calling it an object will be somewhat arbitrary. Different observers may do it in different ways.
- From Cartesian certainty to approximate knowledge

The challenges of the 21st century, characterized by ‘manufactured risk’ such as the BP Deepwater Horizon accident, Fukushima Daiichi and terrorism, manifests as an ‘anticipation’ of catastrophic consequences that stretches the boundaries of time and space and thereby challenges notions of security and safety by ‘…corroding the security guarantees formerly provided by the basic institutions of the nation-state’ (Beck 2009). Following 9/11, according to Coaffee and Wood (2006), the “rings of steel” security paradigm appeared inadequate, thereby requiring a shift in mental models to a security policy that was both proactive and pre-emptive, and in which embraced ‘active anticipation and “reflexive” risk management strategies’ (the hallmark of the risk society).

Similarly, events such as the BP Deepwater Horizon oil disaster, Fukushima Daiichi nuclear meltdown highlight the manufactured risks that shape the emergence of the risk society and links to economic, environmental, food, health security (Masys 2012a, 2012b; Masys et al. 2014).

Aradau and van Munster (2007: 93) reports that ‘…in conditions of extreme uncertainty, decision-makers are no longer able to guarantee predictability, security and control’. The network model perpetuates this and highlights our inability to understand the complex interdependencies that exist and their influence with regards to emergent behaviour. The Cartesian-Newtonian notion of linear causality no longer applies. Our reductionist view is no longer sufficient to understand risk and hazards. They are now nonlinear, interdependent and contagion rapid.

Addressing security concerns at the ‘sharp end’ presents an illusion of impact and influence. To address the underlying security challenges requires a ‘rhizomal’ (Masys 2010, 2012a, 2012b) strategy that considers the nonlinearity and complexity. Drawing from complexity theory, Dekker, Cilliers and Hofmeyr (2011: 941) argue that ‘… analytic reduction cannot tell how a number of different things and processes act together when exposed to a number of different influences at the same time. This is complexity, a characteristic of a system. Complex behavior arises because of the interaction between the components of a system. It asks us to focus not on individual components but on their relationships’. From Beck’s risk society to network thinking, we move from crisis management to complexity management (Masys 2014). We thereby characterise manufactured risks as those hyper-risks that are seeded into a highly interdependent and interconnected network.

For example, as described in Masys et al. (2014) 'The DIET Report Executive summary (2013: 9) argues that although the earthquake and tsunami of March 11 2011 are considered triggers of the cataclysmic event, 'the subsequent accident at the Fukushima Daiichi Nuclear Power Plant cannot be regarded as a natural disaster. It was a profoundly manmade disaster—that could and should have been foreseen and prevented'. Similarly, the recent Ebola outbreak represents an example of the transborder and global effects stemming from a health security matter. As described by Kalra et al. (2014: 164) the Ebolavirus was first reported in the 1970s in remote villages of Africa. *Ebolavirus* (EBOV) causes a severe, frequently fatal hemorrhagic syndrome in humans. The effects stemming from the outbreak are not only physiological but also perpetuates fear and economic turmoil among the local and regional populations in Africa. 'The 2014 Ebola outbreak in Western Africa has been the most severe in history and was declared a public health emergency by the World Health Organization. Given the widespread use of modern transportation and global travel, the EBOV is now a risk to the entire Global Village, with intercontinental transmission only an airplane flight away' (Kalra et al. 2014: 164).

The anticipation of new threats associated with health security resonates with terrorism. Beck (2009) argues that '…the anticipation of new kinds of threats emanating from (deliberate) terrorist attacks represent a persistent public concern. With this, risk becomes the cause and medium of social transformation' and thereby shapes the security agenda. Mythen and Walklate (2006: 124) argue that 'the nature of 'new terrorism' has created and have themselves impacted upon both public opinion and the formation of domestic and international security policy'. This new terrorism is characterized to be '…more threatening to human life, with active terrorist cells seeking to launch unannounced and spectacular high-lethality acts which directly target civilians' (Mythen and Walklate 2006: 126).

From the notion of anticipation, resilience, as a security posture emerges as the ability to detect, prevent and if necessary handle disruptive challenges whether natural or man-made. This includes but is not limited to disruptive challenges arising from the possibility of a terrorist attack. Many elements of response to natural disaster require a similar capability to those of a terrorist attack, and vice versa.

4 Networking Thinking and Risk Society (A Networked Risk Model)

Reconciling Becks risk society and network thinking, the distinction between 'natural hazards', man-made disasters and 'manufactured risks' must be recast as interdependent hyper/hybrid risks. With events like the Ash cloud (2010) and Fukushima Daiichi nuclear accident, natural and man-made risks become blurred. Hyper-risks and hybrid risks emerge. Safety and security risks become transborder and transnational arising from their inherent interdependency and interconnectivity.

Terrorism, for example, challenges our notion of time and space regarding our ability to ensure safety and security. As Beck argues, 'the only viable way of ensuring national security is to nurture transnational security networks (Beck 2002: 47)' (Mythen 2007: 805). This approach resonates with comprehensive approaches pertaining to cyber security described in Masys (2014).

The manufactured global interdependencies make local natural disasters highly relevant globally shaping and affecting global supply chains and as such economic security, food security, energy security. The high consequence risks that threaten public and private life in the risk society are no longer random products of external nature, but rather, are an unanticipated and unintended consequence of our actions and lack of networked understanding of hyper risks.

The hyper risk cross geospatial and geopolitical boundaries emerging as global risks of a cosmopolitan society that evade the boundaries of state sovereignty and national security (Ekberg 2007: 352). This has significant effects on how we conceptualize security. What emerges is a new formulation of risk and security that recasts Becks risk society model in terms of hyper risks stemming from hyper-connectivity. The networked risk model thereby becomes more than a theoretical construct but facilitates an approach to manage complexity (Barabasi 2003, 2013). Like Becks risk society, the network risks are about complexity, anticipation and uncertainty.

The framework of global risk society under the interpretation of networked thinking and hyper risks now accommodates crime, migration or human trafficking, as risks. The pervasiveness of the cyber domain in supporting organized crime resonates with the notion of manufactured risks. It is through these underlying networks that Helbing (2013: 51) argues that we have '…created pathways along which dangerous and damaging events can spread rapidly and globally' and thereby has increased systemic risks.

5 Conclusion

The 'networked' understanding of hyper-risks (Helbing 2013) requires a more holistic approach to hazard identification and risk management that transcends the linear agent-consequence analysis. We see how 'networked risks' are not confined to national borders or a single sector, and do not fit the monocausal model of risk. As argued by Renn et al. (2011: 234) such risks or hyper-risks are '…complex (multi-causal) and surrounded by uncertainty and/or ambiguity'.

This is about complexity framing. Beck (1992) risk discourse regarding manufactured risks and effects that are both temporally and spatially displaced resonates with the complexity notion of nonlinearity. Hence the inherent interdependencies and interconnectivity that characterizes the risk space leads to a network model. The notion of hyper-risks (Helbing 2013; Masys et al. 2014) captures well the interconnectivity and complexity of the security threats. The complexity lens thereby becomes prominent in examining security.

The lessons learned from such events as 9/11 and 7/7, Ebola, financial crisis, have shaped the safety and security agenda. This stage of anticipation regarding disasters and catastrophes require a stance of sensemaking, prevention and resilience. In this sense, the risk discourse is made present in the hearts and minds of the public by the 'anticipation' of events such as the BP Deepwater Horizon and terrorism and the omnipresence of the manufactured risks as a risk and emergency management strategy. High impact low probability events (black swans) (Masys 2012a, 2012b; Masys et al. 2014) highlights the expectation of the unexpected and emerged as the new risk paradigm shaping new possibilities for actions. The transborder effects of crime, terrorism, extreme weather, NATECH (Fukushima) shows that national security is no longer national security (Beck 2002).

References

Aradau C, van Munster R (2007) Governing terrorism through risk: taking precautions, (un)knowing the future. Eur J Int Relat 13(1):89–115

Barabasi A-L (2003) Linked. Plume, Penguin Group, New York

Barabasi A-L (2013) Network science. Phil Trans R Soc A 371:20120375. Published 18 Feb 2013. http://rsta.royalsocietypublishing.org/content/roypta/371/1987/20120375.full.pdf

Barnett J (2013) Environmental security. In: Collins A (ed) Contemporary security studies, 3rd edn. Oxford Press, Oxford

Beck U (1992) Risk society: towards a new modernity. Sage, London

Beck U (2002) The terrorist threat: world risk society revisited. Theory Cult Soc 19(4):39–55

Beck U (2003) The silence of words: on war and terror. Secur Dialogue 34(3):255–267

Beck U (2009) World at risk. Polity Press, Cambridge

Capra F, Luisi PL (2014) The systems view of life: a unifying vision. Cambridge University Press, Cambridge

Coaffee J, Wood DM (2006) Security is coming home: rethinking scale and constructing resilience in the global urban response to terrorist risk. Int Relat 20(4):503–517

Dekker S, Cilliers P, Hofmeyr J-H (2011) The complexity of failure: implications of complexity theory for safety investigations. Saf Sci 49:939–945

DIET Report Executive Summary (2013) https://www.nirs.org/fukushima/naiic_report.pdf

Ekberg M (2007) The parameters of the risk society. Curr Sociol 55(3):343–366

Emmers R (2013) Securitization. In: Collins A (ed) Contemporary security studies, 3rd edn. Oxford University Press, Oxford

Harris AJL, Gurioli L, Hughes EE, Lagreulet S (2012) Impact of the Eyjafjallajökull ash cloud: a newspaper perspective. J Geophys Res 117(B00C08):1–35

Helbing D (2013) Globally networked risks and how to respond. Nature 497:51–59

Johnson CW (2008) Understanding failures in international safety infrastructure: a comparison of European and North American power failures. In: Proceedings of the 26th international conference on system safety, Vancouver, BC, 25–29 Aug 2008

Kalra S, Kelkar D, Galwankar SC, Papadimos TJ, Stawicki SP, Arquilla B, Hoey BA, Sharpe RP, Sabol D, Jahre JA (2014) The emergence of Ebola as a global health security threat: from 'Lessons Learned' to coordinated multilateral containment efforts. J Glob Infect Dis 6(4):164–177. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4265832/?report=classic

Kroger W, Zio E (2011) Vulnerable systems. Springer Publishing, Dordrecht

Masys AJ (2010) Opening the black box of human error: revealing the complex aetiology of fratricide. VDM Publishing, Germany

Masys AJ (2012a) The emergent nature of risk as a product of 'heterogeneous engineering—a relational analysis of the Oil and gas industry safety culture. In: Bennett S (ed) Innovative thinking in risk, crisis and disaster management. Gower Publishing, UK

Masys AJ (2012b) Black swans to grey swans—revealing the uncertainty. Int J Disaster Prev Manage 21(3):320–335

Masys AJ (2013) Human security—a view through the lens of complexity. In: Gilbert T, Kirkilionis M, Nicolis G (eds) Proceedings of the European conference on complex systems 2012. Springer Proceedings in Complexity, pp 325–335

Masys AJ (2014) From crisis management to complexity management: HA/DR by design. In: 12th Japan-Canada security symposium for peace and security cooperation, Tokyo, Japan, 9–10 June 2014

Masys AJ, Ray-Bennett N, Shiroshita H, Jackson P (2014) High impact/low Frequency extreme events: enabling reflection and resilience in a hyper-connected world. In: 4th International conference on building resilience, 8–11 Sept 2014, Salford Quays, United Kingdom (Proc Econ Finance 18:772–779)

Masys AJ (2015) Promoting the network mindset to support humanitarian crisis management: towards prediction, prevention and resilience. In: Proceedings of the international conference on resilience, research and innovation, 26–28 Oct 2015, Djibouti. http://www.rri.dj/

Mythen G (2007) Reappraising the risk society thesis: telescopic sight or myopic vision. Curr Sociol 55(6):793–813

Mythen G, Walklate S (2006) Communicating the terrorist risk: harnessing a culture of fear? Crime Media Cult 2(2):123–142

Mythen G, Walklate S (2008) Terrorism, risk and international security: the perils of asking what if? Secur Dialogue 39(2–3):221–242

Raphael S, Stokes D (2013) Energy security. In: Collins A (ed) Contemporary security studies, 3rd edn. Oxford Press, Oxford

Rasmussen M (2001) Reflexive security: NATO and international risk society. Millennium 30 (2):285–309

Renn O, Klinke A., van Asselt M (2011) Coping with complexity, uncertainty and ambiguity in risk governance: a synthesis. AMBIO, 40: 231–246

Senge PM (1990) The fifth discipline: the art and practice of the learning organization. Century Business, London

Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee (2015) http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

UNHCR (2015) http://www.unhcr.org/pages/49e486a76.html

Urry J (2002) 'The Global Complexities of September 11th' Theory, Culture and Society 19(4): 57–69

Vespignani A (2009) Predicting the behavior of techno-social systems. Science 325:425–428

Vespignani A (2010) The fragility of interdependency. Nature 464:984–985

Washington Post (2015) 3 ways the Fukushima nuclear disaster is still having an impact today (March 12). https://www.washingtonpost.com/news/worldviews/wp/2015/03/12/3-ways-the-fukushima-nuclear-disaster-is-still-having-an-impact-today/

Wattie J, Masys AJ (2014) Enabling resilience: an examination of high reliability organizations and safety culture through the lens of appreciative inquiry. In: Masys AJ (ed) Disaster management—enabling resilience. Springer, Berlin

WEF (2015) Global Risks 2015, 10th edn, insight report

Xu T, Masys AJ (2015) Critical infrastructure vulnerabilities: embracing a network mindset. In: Masys AJ (ed) Exploring the security landscape: non traditional security challenges. Springer, Berlin