Cybersecurity in the European Union

Resilience and Adaptability in Governance Policy

George Christou

New Security Challenges Series

General Editor: **Stuart Croft**, Professor of International Security in the Department of Politics and International Studies at the University of Warwick, UK, and Director of the ESRC's New Security Challenges Programme

The last decade demonstrated that threats to security vary greatly in their causes and manifestations, and that they invite interest and demand responses from the social sciences, civil society and a very broad policy community. In the past, the avoidance of war was the primary objective, but with the end of the Cold War the retention of military defence as the centrepiece of international security agenda became untenable. There has been, therefore, a significant shift in emphasis away from traditional approaches to security to a new agenda that talks of the softer side of security, in terms of human security, economic security and environmental security. The topical *New Security Challenges Series* reflects this pressing political and research agenda.

Titles include:

Angela Pennisi di Floristella
THE ASEAN REGIONAL SECURITY PARTNERSHIP
Strengths and Limits of a Cooperative System

Natasha Underhill
COUNTERING GLOBAL TERRORISM AND INSURGENCY
Calculating the Risk of State-Failure in Afghanistan, Pakistan and Iraq

Abdul Haqq Baker
EXTREMISTS IN OUR MIDST
Confronting Terror

Robin Cameron
SUBJECTS OF SECURITY
Domestic Effects of Foreign Policy in the War on Terror

Sharyl Cross, Savo Kentera, R. Craig Nation and Radovan Vukadinovic (*editors*)
SHAPING SOUTH EAST EUROPE'S SECURITY COMMUNITY FOR THE TWENTY-FIRST CENTURY
Trust, Partnership, Integration

Tom Dyson and Theodore Konstadinides
EUROPEAN DEFENCE COOPERATION IN EU LAW AND IR THEORY

Håkan Edström, Janne Haaland Matlary and Magnus Petersson (*editors*)
NATO: THE POWER OF PARTNERSHIPS

Håkan Edström and Dennis Gyllensporre
POLITICAL ASPIRATIONS AND PERILS OF SECURITY
Unpacking the Military Strategy of the United Nations

Håkan Edström and Dennis Gyllensporre (*editors*)
PURSUING STRATEGY
NATO Operations from the Gulf War to Gaddafi

Hamed El-Said
NEW APPROACHES TO COUNTERING TERRORISM
Designing and Evaluating Counter Radicalization and De-Radicalization Programs

Philip Everts and Pierangelo Isernia
PUBLIC OPINION, TRANSATLANTIC RELATIONS AND THE USE OF FORCE

Adrian Gallagher
GENOCIDE AND ITS THREAT TO CONTEMPORARY INTERNATIONAL ORDER

Kevin Gillan, Jenny Pickerill and Frank Webster
ANTI-WAR ACTIVISM
New Media and Protest in the Information Age

Ellen Hallams, Luca Ratti and Ben Zyla (*editors*)
NATO BEYOND 9/11
The Transformation of the Atlantic Alliance

Christopher Hobbs, Matthew Moran and Daniel Salisbury (*editors*)
OPEN SOURCE INTELLIGENCE IN THE TWENTY-FIRST CENTURY
New Approaches and Opportunities

Janne Haaland Matlary
EUROPEAN UNION SECURITY DYNAMICS
In the New National Interest

Sebastian Mayer (*editor*)
NATO'S POST-COLD WAR POLITICS
The Changing Provision of Security

Michael Pugh, Neil Cooper and Mandy Turner (*editors*)
WHOSE PEACE? CRITICAL PERSPECTIVES ON THE POLITICAL ECONOMY OF PEACEBUILDING

Aglaya Snetkov and Stephen Aris
THE REGIONAL DIMENSIONS TO SECURITY
Other Sides of Afghanistan

Aiden Warren and Ingvild Bode
GOVERNING THE USE-OF-FORCE IN INTERNATIONAL RELATIONS
The Post 9/11 Challenge on International Law

George Christou
CYBERSECURITY IN THE EUROPEAN UNION
Resilience and Adaptability in Governance Policy

New Security Challenges Series
Series Standing Order ISBN 978–0–230–00216–6 (hardback) and
ISBN 978–0–230–00217–3 (paperback)
(*outside North America only***)**

You can receive future titles in this series as they are published by placing a standing order. Please contact your bookseller or, in case of difficulty, write to us at the address below with your name and address, the title of the series and the ISBNs quoted above.

Customer Services Department, Macmillan Distribution Ltd, Houndmills, Basingstoke, Hampshire RG21 6XS, England

Cybersecurity in the European Union

Resilience and Adaptability in Governance Policy

George Christou
Associate Professor of European Politics, University of Warwick, UK

palgrave
macmillan

Softcover reprint of the hardcover 1st edition 2016 978-1-137-40051-2

First published 2016 by
PALGRAVE MACMILLAN

Palgrave Macmillan in the UK is an imprint of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire RG21 6XS.

Palgrave Macmillan in the US is a division of St Martin's Press LLC, 175 Fifth Avenue, New York, NY 10010.

Palgrave Macmillan is the global academic imprint of the above companies and has companies and representatives throughout the world.

Palgrave® and Macmillan® are registered trademarks in the United States, the United Kingdom, Europe and other countries.

ISBN 978-1-349-55790-5 ISBN 978-1-137-40052-9 (eBook)

DOI 10.1057/9781137400529

This book is printed on paper suitable for recycling and made from fully managed and sustained forest sources. Logging, pulping and manufacturing processes are expected to conform to the environmental regulations of the country of origin.

A catalogue record for this book is available from the British Library.

A catalog record for this book is available from the Library of Congress.

Contents

Tables, Boxes and Figures

Tables

Boxes

Figures

Foreword

Today's private and business life depends critically on modern information and communication technologies (ICTs). Social networks, information retrieval, shopping, supply chains, everything is done on the Internet. Global cyberspace becomes a small virtual village with no borders. While on the one hand new business models create jobs and economic growth, these are often associated with new risks: cybercrime, cyberespionage, cybersabotage and cyberwarfare. Cyber threats need to be addressed and ICT security awareness and security solutions are needed. In addition, we need a new governance structure in this cyberspace. Different ethical and cultural backgrounds in America, Europe and Asia make it difficult to find a common code of conduct in this brave new cyber world.

The European Union of 28 member states has been a success story over the last decades in terms of market harmonisation and economic growth. However, the 2009 financial crisis, youth unemployment and similar social issues are challenges that Europe still faces. In this context, the Digital Single Market Strategy of the European Commission published this year is a strong commitment for Europe becoming a global competitive leader in ICTs. The security and availability of ICTs is of increasing concern and privacy is becoming an important issue in a world where nothing is forgotten on the net. We see a growing number of security and data breaches and cybercrime becomes a 'business'.

The European Commission has taken several initiatives to improve the situation, such as the Network and Information Security Agenda in 2001, the first ePrivacy Directive in 2002, the establishment of ENISA in 2004, the Critical Information Infrastructure Communication in 2009, the Digital Agenda for Europe in 2010 and the EU Cybersecurity Strategy in 2013. But what impact did it achieve? We have awareness among political leaders and industry CEOs and Computer Emergency Response Teams in all 28 member states. Most member states have national cybersecurity strategies. But we still do not have an overall EU governance framework for network and information security, overall incident reporting (like in the telecommunication sector) and trusted communication on threats and attacks. The NIS directive, which is currently under negotiation between the European Parliament and the European Council, aims to overcome these issues. One hurdle is still

that cybersecurity is often seen as part of national security, thus falling under national sovereignty. So there is still a long way to go before we have a secure and open cyberspace in Europe.

This book, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, by George Christou comes at just the right moment. It accepts the challenge of describing and analysing the European Union's state of play on cybersecurity and provides a deeper understanding of how the EU can achieve effective security resilience. Christou describes the EU's ecosystem of cybersecurity governance and to what extent the EU achieves a comprehensive approach to cybersecurity within the EU ecosystem. In addition, he outlines what conditions are needed for effective security and resilience. Christou shows that cybersecurity is the basis for Europe's social and cultural benefits as well as for our economic growth. He demonstrates that ICT security is critical to achieve this.

Today politicians often still think and act in silos: cyberwar is defence, cybercrime is law enforcement, privacy is justice, and so on. The technology and the attackers do not distinguish between these different areas. Was the Stuxnet attack cybercrime? Cybersabotage? Cyberwarfare? Depending on the political interpretation it can be different, but the attackers do not care. And next time the same Stuxnet technology – which is now publicly known – can be used for attacking an automotive plant or a denial of service attack on a critical infrastructure, or for cyberblackmailing. Therefore all actors and stakeholders have to work in a cooperative manner, and for this, processes such as incident reporting and information sharing are key.

Christou's achievement is that he presents us with the global cyberpicture and analyses the EU–US relationship and the national interests (for example, the UK); he addresses cybercrime as well as cyber-defence, and at the end discusses the question: is 'security as resilience' the solution?

The message of the book – and I fully share this – is: 'Fostering trust and security in cyberspace is not an option for the EU; it is a requirement and pre-requisite for realising its own ambitions, promoting its values, and (re)defining its identity in a dynamic global order that is increasingly reliant on digital interoperability and connectivity.'

Enjoy reading it!

Prof. Udo Helmbrecht
Executive Director
European Network and Information Security Agency

Preface

Securing cyberspace has become one of the most pressing security challenges of the twenty-first century through its importance to everyday life for government, business and citizens alike. The cyber world and its associated technologies have, on the one hand, created many social, cultural, economic and political opportunities for all, whilst on the other, its borderless nature has brought with it threats in the form of cyber-attacks and cybercrime. The European Union (EU) is not immune to such threats. The Distributed Denial of Service attacks on Estonia's public and private networks and systems in 2007, and attacks on its own institutions in 2011, among other high-profile cases, provided a wake-up call for the EU and ensured that cybersecurity moved swiftly up the EU's political agenda. The EU subsequently produced its first Cybersecurity Strategy in 2013 to prioritise and integrate its policies and actions internally and externally; well aware that the EU could not address cybersecurity challenges alone given the global and open nature of the Internet.

Within a broader international, regional and national context, this book will analyse the EU's approach to the challenges it faces in cyberspace, before and following the publication of its Cybersecurity Strategy. Utilising and fusing the concepts of resilience and security governance, it offers a novel framework for understanding and assessing how far the EU has progressed in embedding the necessary conditions for a resilient and secure cyber ecosystem to emerge in Europe and beyond. It is argued that embedding such conditions will facilitate the emergence of an adaptable and flexible resilience needed for the EU to foster security, confidence and trust in cyberspace. This is not an option for the EU and its citizens but rather a pre-requisite for realising its own ambitions, promoting its values and (re)defining its identity in a dynamic global order that is increasingly reliant on digital interoperability and connectivity.

Acknowledgements

I would like to express my thanks to colleagues in the Department of Politics and International Studies at the University of Warwick that have offered positive encouragement throughout the process of researching and writing this book. I am particularly grateful to Stuart Croft, Chris Hughes, Mat Watson, Shaun Breslin, Richard Aldrich, Mike Smith, Nick Vaughan-Williams, Chris Moran, Oz Hassan and Chris Browning for their support in discussing the ideas in the book and, more generally, for providing the time and space for me to converse with them when writing progression was not always at its peak! I would also like to thank colleagues in the Cyber Team in WMG at Warwick, and in particular Tim Watson and Carsten Maple for very helpful discussions on different aspects of the research, and for pointing me in the right direction with regard to people that I could engage with in government and industry that helped to fill gaps in my information as the book evolved. I would also like to extend my thanks to the commissioning editors at Palgrave, Eleanor Davey Corrigan and Hannah Kašpar, for their guidance, advice and above all patience with me in delivering the final manuscript.

Much of the research conducted in the writing of this book would not have been possible without the funding received from the European Commission for the large Framework 7 project, *Global Reordering: Evolution of European Networks* (GR:EEN), and for this I am very grateful. I would also like to extend my thanks to the many experts and officials that agreed to speak to me about my research along the way; our conversations helped me to clarify many aspects of the EU's evolving cybersecurity strategy, policies and practices. Special thanks go to Kyriakos Revelas in the European External Action Service for his friendship and consistent support whilst writing the book, as well as to Udo Helmbrecht and his staff at the European Network and Information Security Agency and Alessandra Falcinelli in DG Connect at the European Commission. Their willingness to facilitate my research at key stages was very much appreciated. I also benefited enormously from interacting with many public and private stakeholders and experts as an active participant of the EU's Network and Information Security Platform. Not only did this provide me with great insight but it also helped me tremendously in confirming some of my assertions and nuancing others throughout the research process.

In addition, I have benefited from positive feedback on presentations of different elements of the book at conferences organised by the University Association for Contemporary European Studies and International Studies Association, as well as various cybersecurity and cybersecurity-related workshops in the UK and in Brussels.

Finally, and above all, thanks to my family for their constant encouragement and in particular to Allison, Constantino and Andreas for their love, understanding and support throughout the duration of this project.

1
Introduction

The salience of cybersecurity in the European Union

Information and communications technologies (ICTs), in particular the Internet, have been an increasingly important aspect of global social, political and economic life for two decades, and are the backbone of the global information society today. Their evolution and development have brought many benefits for individuals, as well as a plethora of public and private institutions and actors; witness the positive impact of social networks on the uprisings in the Arab Spring in 2011, or the increased use of e-commerce across business and individuals. ICTs have also, however, brought the threat of serious cyber-attacks demonstrated in recent years through acts of cyber espionage and cybercrime within the virtual, networked ecosystem that we live in.

These have included, to name but a few high-profile cases, attacks on Estonia's public and private institutions in 2007, Russian-sourced attacks on Georgian systems in 2008, the Stuxnet worm attack on the Iranian nuclear programme in 2009, the re-routing by a Chinese Internet service provider (ISP) of sensitive US government e-mail traffic to China, the WikiLeaks affair in 2010, not to mention attacks on several EU institutions in 2011 (the European Commission, the European Parliament). Beyond such high-profile attacks, reports of attacks on companies have also proliferated in the last few years (Net Losses Report 2014). Such events have underlined the vulnerability of ICTs and brought to the fore important policy issues that permeate the information security agenda. They have also highlighted the global and multi-dimensional nature of the information assurance problem – with recognition that security governance developed to combat the cyber threat must engage the many levels, actors, institutions and individuals involved within the cyber ecosystem.

In this context, the European Union (EU) over the past ten years has been developing its policies towards cyber threats, even though this has often been quite fragmented. The EU's Internal Security Strategy (ISS, November 2010) and the Digital Agenda for Europe (2010) have provided the main broad guidance for its activities in this area in more recent times. However, the EU also produced more specific proposals through the European Strategy for Internet Security (ESIS 2011) and the Cybersecurity Strategy for the European Union (EUCSS 2013).

Institutionally, the European External Action Service (EEAS) plays the role of central coordinative node in agreeing on and projecting EU cybersecurity policy externally, whilst the EU Computer Emergency Response Team (CERT) fulfils the technical aspects of such a role internally. The Directorate Generals Connect (DG Connect) and Home (DG HOME) take the lead in developing policy in relation to Network and Information Security (NIS) and cybercrime, respectively, with the European Parliament also playing a key role within the policy process with regard to relevant Regulations and Directives. Beyond this, there are key EU agencies, including the European Defence Agency (EDA) which works on developing EU cyber defence, the European Network and Information Security Agency (ENISA) which works with relevant stakeholders to develop advice and recommendations on good practice in information security (including cybercrime), and with EU member states in implementing relevant EU legislation to improve the resilience of Europe's critical information infrastructure and networks. Finally, Europol, and specifically the European Cybercrime Centre (EC3), focuses on the operational and strategic aspects of cybercrime (see Figure 1.1).

Cybersecurity is certainly one of the most salient problems on the EU's political agenda, made even more pressing after cyber-attacks on the European Parliament, and the EU Commission and the EU's Emissions Trading Scheme in March 2011, the latter at an approximate cost of €30 million in stolen emissions allowances (Leyden 2011). The estimated cost of cybercrime to the EU is €85 billion annually (EU prepares to launch first cybercrime centre, 2012) and certain analysts further estimate that within Europe up to 150,000 jobs could be lost to cybercrime over the next few years, in addition to the damage done to trade, competitiveness, innovation and economic growth (Net Losses Report 2014).

Such problems are not easily resolvable given their complex, often ambiguous and cross-jurisdictional nature, and the EU, although certainly making progress in the evolution of its policies in these areas,

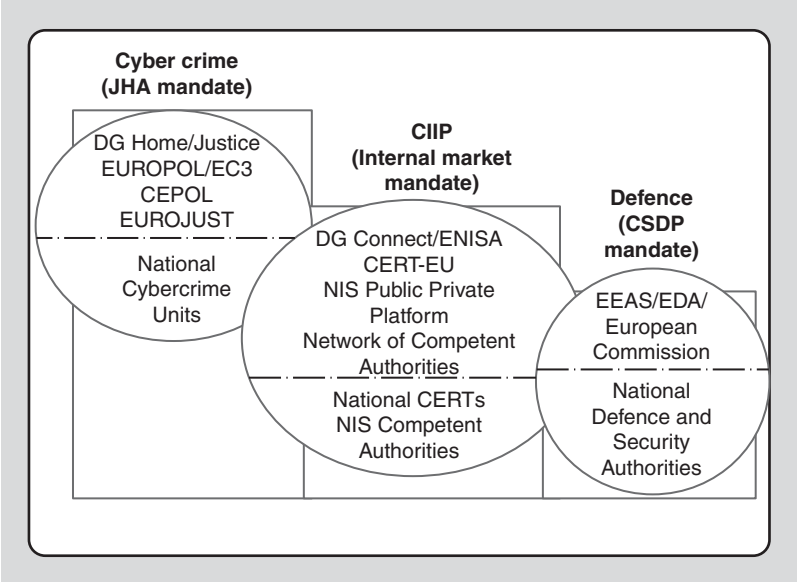

Figure 1.1 The central pillars of the EU Cybersecurity Strategy (2013)
Source: Compiled from data within the Cybersecurity Strategy of the EU (2013, p.17).

still has a long way to go before it can claim to have a unified, effective and resilient ecosystem for governing cyber threats. Indeed, whilst creating a comprehensive approach to cybersecurity within the EU has become a political priority with a renewed sense of urgency around the issue, there is still a lack of clarity on how cyber threats can be regulated and coordinated in governance terms in order to build sustainable and resilient platforms and systems. In short, whilst the EU certainly possesses many tools and mechanisms for addressing the cybersecurity issue, how it uses them needs to be developed, and the consistency and coherence across the institutions and actors involved improved, in what can only be described as an evolutionary security governance ecosystem.

Central questions and objectives of the book

It is the purpose of this book, therefore, to explain the evolution of the EU governance system for cybersecurity and provide a deeper understanding of how the EU can construct an effective security as resilience (see Chapter 2) with regard to questions of cyber threat. Moreover, it

will facilitate provision of the answer to the central questions that this book seeks to ask:

- How can we characterise and understand the EU's evolving ecosystem of cybersecurity governance?
- To what extent has the EU been able to construct a comprehensive approach to cybersecurity within the evolving ecosystem, and embed the necessary conditions for effective security as resilience?
- What is the nature of the resilient ecosystem emerging in the EU?

What is at stake within the EU space is significant. If the EU cannot facilitate the construction of the necessary conditions for security as resilience in cyberspace in the near and long term, then there is a danger that trust and confidence in the Internet will be eroded, and that the EU will remain vulnerable to cyber-attack and, importantly, unable to react and recover in an effective way. Improving the way in which the EU does cybersecurity is essential for the continued social, economic, financial and cultural benefits that citizens and businesses derive from the Internet and, more broadly, evolving ICTs. Moreover, it is critical if it is to achieve the objectives it has set for itself in the Digital Agenda for Europe (2010), and equally as significant, the driving force of such an agenda, the Europe 2020 strategy. Fostering trust and security in cyberspace then is not an option for the EU; it is a requirement and prerequisite for realising its own ambitions, promoting its values and (re)defining its identity in a dynamic global order that is increasingly reliant on digital interoperability and connectivity.

Theoretically and conceptually, work has been sparse in relation to analysing the EUCSS and emerging cybersecurity ecosystem. Broader research on cybersecurity has progressively increased from different perspectives (see Chapter 1), and certain authors have offered some insight into the EU approach through deploying the concepts of cyber power (Klimburg and Tirmaa-Klaar 2011; Sliwinski 2014) and resilience (Miriam Dunn Cavelty 2013). However, such works have not been comprehensive in their coverage or conceptual reflection on the emergent ecosystem of resilience within the EU and Europe. I am not arguing here that such approaches do not have anything to offer, in fact quite the opposite. Such works need further application and development if we are to reach a deeper understanding of how far the EU has travelled towards achieving effective security as resilience within its evolving ecosystem. The argument in this book is that an adaptable and flexible

type of resilience should drive the EU's approach to cybersecurity – that is, the EU should focus on developing the conditions for effective cybersecurity as resilience, through appropriate governance modes and mechanisms, for it to become an influential actor in cyberspace and a leader with regard to good practice in cybersecurity and its many different dimensions (see Chapters 2 and 6).

Given the above context, the objectives of the book are threefold:

- To provide a conceptually driven and comprehensive analysis of the EU's emerging ecosystem for cybersecurity
- To employ a novel conceptual framework to the issue of EU cybersecurity through a fusion of resilience and security governance literatures
- To produce a deeper understanding of progress in the development of the EU's approach and strategy to cybersecurity and the implications this has for effective cybersecurity as resilience in Europe and beyond

It is the contention of the author that such an undertaking is both timely and necessary, in particular given the hitherto lack of attention to the EU's evolving practice in cybersecurity in an era of both internal institutional change and transition following ratification of the Lisbon Treaty (2009), and increasing security challenges in cyberspace, whereby citizens, governments, business and other actors are increasingly threatened (perceived or real) – culturally, financially, economically, politically and strategically. Whilst there are certainly many ideas 'out there' evolving through deliberation and discussion on what works best for effective cybersecurity, and the European Commission and other EU agencies such as ENISA are proactive in developing common definitions of problems (what is cybersecurity) and solutions (what is meant by resilience, types of public–private partnerships in cybersecurity), this book aims to assess how the main pillars of the EUCSS – cybercrime, network and information security (critical information infrastructure protection) and cyber defence (Chapters 5 and 6) – are working and pulling together to construct a more resilient and common understanding and practice related to cybersecurity. In addition, it seeks to place this in the context of the global more broadly (Chapter 2), and transatlantic cooperation more specifically (Chapter 7). Furthermore, it explores national resilience through offering an in-depth analysis of what is considered an advanced EU member state – the UK – in the area of cybersecurity (Chapter 4).

Certain clarifications need to be added and parameters made clear before outlining the structure of the book. The first relates to what sort of role the EU can realistically play in cybersecurity given that it touches upon many issues of national sensitivity and security. The EUCSS recognises that 'it is predominantly the task of member states to deal with security challenges in cyberspace' (EUCSS 2013, p.4), but also that the EU has a key role to play as an actor in itself. To this end, it is clear that the EU can be a facilitator and platform across the different realms of cybersecurity creating the necessary conditions for an effective culture of cybersecurity to emerge within member states – and critically, working with member states – weak and strong – in order to construct the minimal standards and skills – legal, technical, political, economic, strategic and operational – required for the EU to develop as a resilient actor and ecosystem in relation to cybersecurity. Not only this, the EU can act as an effective regional node for the exchange of good practice across the member states – and internationally, through the evolution, promotion and projection of principles and norms for Internet governance, including critical issues of cybersecurity. Indeed, given the borderless and transnational nature of cybersecurity and the external reach and influence of the EU, it has a critical role to play in creating a culture of resilience and cybersecurity not only in Europe, but also globally.

The second relates to the ongoing debate about how to define cybersecurity and its various dimensions – cybersecurity, cybercrime, cyber espionage, cyber terrorism, cyber hacktivism and so on. Whilst this has become a topic in and of itself for some scholars (see, for example, Di Camillo and Miranda 2011), and many regional and international organisations and agencies provide varied definitions, I do not intend to engage in the debate explicitly within this book. This is not to say that definitions are not important, but rather that any such discussion will be embedded within the relevant analysis and discussion in the themes visited in each chapter. Indeed a central part of the analysis will focus on the emergence (or not) of common definitions and understandings across the different dimensions of cybersecurity, with the starting point being definitions adopted by the EU (including relevant EU agencies) and its member states. Cybersecurity, in this instance, is defined by the EU in broad terms, with the definition of cybercrime much more focused in nature (see Box 1.1). Cyber defence is not defined within the EU documents given the sensitivity among member states on this issue, and the reluctance of certain member states to participate given their own cyber defence strategies (see Chapter 6). This is also why cyber

defence, unlike cybercrime and NIS, falls under the intergovernmental Common Security and Defence Policy (CSDP) mandate and not within the EU's exclusive or shared competence.

Box 1.1 European Union definitions of cybersecurity and cybercrime

Cybersecurity: 'the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein'
Cybercrime: 'a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (for example, fraud, forgery, and identity theft), content-related offences (for example, on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (for example, attacks against information systems, denial of service and malware)'

Source: EU Cybersecurity Strategy (2013, p.3).

Third, whilst the author acknowledges and accepts that the analysis of cybersecurity within any domain must be interdisciplinary for a more comprehensive account to emerge – that is, giving equal weight to the 'physical layer' (hardware), 'logic layer' (software and protocol) and content or 'social layer' (culture, human contact, ideas and policy) (Benkler 1998, 2007) – this book prioritises the latter, with an emphasis on the social and policy conditions for a security as resilience culture to emerge. In this sense, it provides a contextual analysis of policy evolution and security logics, and a contemporary analysis of practice and the implications this has for ensuring an effective security as resilience approach. Thus, those expecting to find in-depth analysis of technological and technical solutions to cybersecurity issues will most likely be disappointed (!); but it is the hope of the author that it will at least create further conversation across the different layers on the relationship

between the policy, cultural and technical challenges of constructing a resilient cybersecurity ecosystem in Europe and beyond. Technical solutions, after all, are only possible if the appropriate legal and policy environment exists to implement them effectively.

Fourth, whilst the book offers comprehensive coverage on what are considered the three main pillars of the EUCSS, there are still many important aspects of EU and European cybersecurity that could not be covered. Thus the book does not delve into the minutiae of EU policymaking and internal cooperation, competition and conflict between EU actors and agencies. In addition, priorities outlined in the EUCSS (2013) such as developing industrial and technological resources for cybersecurity and establishing a coherent international cyberspace policy for the EU are only discussed implicitly throughout the book; with the latter international aspect analysed in depth to some degree with regard to the international context (Chapter 3) and the transatlantic partnership (Chapter 7). Beyond this, issues such as cloud computing security, smart technologies (cities, environment, devices and so on) and IT-enabled industrial control systems, to name but a few, are not covered in order to ensure an element of focus and depth to the central elements within the EUCSS that are analysed. Finally, a choice was made to provide one in-depth country case study (the UK, see Chapter 4) rather than including additional, but less substantive country case studies; although developments within the EU are alluded to in the analysis of the main pillars of the EUCSS. These choices obviously limit the scope of analysis, but with the acknowledgment that not all cyber issues affecting Europe, the EU and its member states could be explored in a single monograph of this type.

Finally, there is one note of caution that needs to be added given the dynamic nature of developments in ICT and cybersecurity policy and practice more broadly, and the formative nature of many of the EU's initiatives stemming from its Cybersecurity Strategy (EUCSS 2013). The reader should be aware that what is offered here, albeit in historical context, is a snapshot of the EU's developments, policies and practices, two years on from the publication of its Cybersecurity Strategy. It is highly probable that by the time this book is published many aspects of the EUCSS and therefore policy and practices will have evolved and changed. It is the ambition of this book though that the analysis offered will provide a context for reflection on the future evolution of the EU's approach and the nature and direction of travel in relation to embedding the necessary conditions for the emergence of a secure and resilient cyber ecosystem in Europe.

The structure and organisation of the book

The aim of this book is to provide a comprehensive and conceptually driven account of the evolution of EU cybersecurity policy and strategy. To this end, Chapter 2 will provide a framework and conceptual markers for understanding the EU's evolving ecosystem of cybersecurity governance. It will review the theoretical literature on cybersecurity more generally and in relation to the EU, and develop a framework for analysis through problematising and fusing the concepts of resilience and security governance. Indeed, this chapter will construct the conceptual argument relating to a *security as resilience* approach, and the basic conditions that would allow this to emerge in the EU and Europe.

Chapter 3 will outline the global context in which the EU operates and interacts in relation to cybersecurity policy. The security of ICTs and the Internet is, by its very nature, borderless, and thus many of the challenges require not just specific EU responses, but coordinated global, public–private responses. Chapter 4 will offer a critical appraisal of the evolution of cybersecurity policy at the national level, focusing on the evolution of cybersecurity policy in a single advanced country, the UK. Whilst the chapter will only provide an in-depth analysis of one EU member state, it will also illuminate progress elsewhere and reflect on good practice that can be potentially transferred within an EU context.

Chapters 5 and 6 then offer in-depth analysis of the EU policies within the three central pillars under scrutiny: cybercrime, NIS and cyber defence. These chapters assess how evolving proposals, logics and practices facilitate the construction of the necessary conditions for security as resilience to emerge, including the differentiated governance mechanisms across the three pillars. Chapter 7 then delves deeper into one of the EU's most important international relationships in relation to cybersecurity and cybercrime: that with the US. This chapter will focus on and analyse the EU–US relationship and its implications for the EU in developing the transatlantic dimension of its Cybersecurity Strategy and ecosystem. More specifically, it will analyse similarities and differences between EU and US logics of security across different issues related to security in cyberspace, in order to assess (a) the extent to which the two partners converge or diverge on critical issues and (b) how this impacts on the creation of a transatlantic security of resilience approach for cybersecurity.

Chapter 8 will summarise the findings and overall implications of the research on the EU in national and global contexts. It will first, assess

how far the EU has travelled in embedding the conditions for a security as resilience approach to emerge; and second, it will offer reflections on the security as resilience approach and emerging governance modes to achieve this in the EU, and a way forward for research and the practice of resilient security in the evolution of the EU's cybersecurity ecosystem.

2
Conceptualising Security as Resilience in Cyberspace

Introduction

Many cybersecurity strategies within and beyond Europe refer to developing effective cyber resilience, but without adequately defining and deconstructing what resilience is, what it looks like at different stages, and the preconditions and governance forms required to achieve it. Approaches to cybersecurity thus far have been theoretically and conceptually eclectic – utilising traditional and critical theories of International Relations (IR) and concepts such as cyber power. This chapter will – in line with the main purpose of this book – draw on existing theorisations of cybersecurity more broadly, and add to them through interrogating resilience and security governance in order to create a holistic approach to assessing the evolution of the European Union's (EU) ecosystem for cybersecurity governance. Moreover, it will seek to provide a frame of reference for not only understanding the 'Internet interconnection system' (ENISA 2011c) but more specifically the conditions that can potentially lead to cybersecurity as resilience across the European space.

Furthermore, this chapter will explore and define the concepts of resilience and security governance and delineate how they will be operationalised in analysing EU cybersecurity. The aim will be to fuse the literature on resilience and security governance in order to construct and establish a security as resilience approach. This will allow the characterisation of emerging governance in the EU Cybersecurity Strategy and more importantly, how this equates to achieving an effective security as resilience in Europe. Whilst such a frame no doubt has synergies with existing conceptual work, it will also add to such literature, not least by introducing different understandings of resilience through which cybersecurity governance can be understood and assessed.

In short, it is the aim of this chapter to provide a framework and conceptual markers for explaining the evolution of the EU governance system for cybersecurity in order to provide a deeper understanding of how the EU can construct an ecosystem of resilient security governance with regard to questions of cyber threat. Such a framework will facilitate provision of a conceptually informed answer to the central questions that this book seeks to ask: How can we characterise and understand the EU's evolving ecosystem of cybersecurity governance? To what extent has the EU been able to construct a comprehensive and resilient approach to cybersecurity within the evolving ecosystem? What is the nature of the resilient ecosystem emerging in the EU? The implicit argument running throughout the chapter and the book is that a more socio-ecological, adaptive and flexible form of resilience should drive the EU's approach to cybersecurity in order for it to become an influential actor in cyberspace and a leader with regards to good practice in cybersecurity and its many different dimensions.

The chapter will be structured as follows to achieve its aim. The first section will provide a contextual overview and assessment of the way in which cybersecurity is theorised and conceptualised in the literature more broadly. The second section will then draw on the specific literature that will be used to construct the framework for the book; namely, resilience and security governance, and sketch out conceptual conditions and markers that can be utilised to understand the development of the EU's emerging ecosystem of cybersecurity. This section will also articulate the relationship between the broader literature and the security as resilience frame constructed for analysis of the EU cybersecurity ecosystem. The final section will summarise the argument made in the chapter and the implications this has for the analysis in the book.

Approaches to analysing cybersecurity

Theoretically informed work on cybersecurity is surprisingly sparse, although growing rapidly. What does exist is focused on the US and other geographical areas (for example, see Kshetri 2013 on the Global South), with no comprehensive, theoretically driven analysis of the EU in cybersecurity. In terms of the existing literature a variety of approaches have been used to analyse the topic, ranging from traditional national strategic and managerial approaches (Libicki 2007, 2009; Janczewski and Colarik 2007; Mehan 2008; Janczewski 2008; Clarke and Knake 2010), to historical approaches (Carr 2009) and 'terrorist' oriented approaches (Verton 2003; Colarik 2006; Wiemann

2006). Such approaches have had little theoretical input and focus more on the real and present danger of cyber threats and potential management of the risks associated with them; in other words, on how to fight the cyber enemy or achieve the 'cyber peace' (Clarke and Knake 2010). More conceptually, methodologically, and theoretically informed works have employed governance (regulatory) approaches (Brown and Marsden 2007; Mueller 2010), pragmatic, eclectic, comparative approaches (Karatzogianni 2006, 2009; Eriksson and Giacomello 2010), innovative mixed-method approaches (Deibert et al. 2012), cyber power approaches (Kramer et al. 2010; Nye, Jr 2010; Klimburg 2011a; Betz and Stevens 2011; Sliwinski 2014[1]) and more critical approaches that attempt to assess the extent to which cyber policy has become securitised (Eriksson 2001; Bendrath et al. 2007; Dunn Cavelty 2007, 2008). These latter works are important for contextual purposes, but also for the fact that much of the work, on governance for example, is intellectually pertinent to the approach taken here in analysing the EU's evolving ecosystem of cybersecurity governance. It is to these works that I will now turn in this section.

Karatzogianni (2009) usefully focuses on how to conceptualise the role of new media in cyber conflict, but there is no real theoretical engagement in the politics of cybersecurity *per se*, and no direct focus on the EU. Whilst not focusing on the EU either, Eriksson and Giacomello (2010, p.3–11) do engage with the literature on the digital age and security – and note in particular that it has largely ignored either 'security' or 'theory'. The Information Society (IS) literature (Castells 1996, 1997, 1998; Mowlana 1997), they suggest, has not focused on state and societal security, but rather, that of the firm and market. At the same time, what they have called digital-age security literature is policy focused and therefore neglects theorisation of cybersecurity; indeed, they conclude that much work within this area is prone to sensationalise the problems posed by cyber threats (the 'electronic Pearl Harbour' scenario), thus potentially over-exaggerating the tools necessary to address issues related to the day-to-day process of information assurance.

What they argue, fundamentally, is that there is a gap between IR theory and security in the digital age, and they subsequently outline the utility of Realism, Liberalism and Constructivism for understanding and explaining security in the digital age before concluding that a 'pragmatic' approach aiming for typological not universal propositions offers a way of utilising insights from different literatures. Interestingly, they demonstrate that liberalism and constructivism are the most relevant IR theories: the former with its emphasis on transnational non-state actors, networked communities, 'vulnerable interdependence' and an emphasis

on the permeability of the boundaries of state; the latter allowing for deeper analyses of discourse, rhetoric, symbols and identity in digital age security.

Such a pragmatic approach is utilised by authors to analyse the politics of threats and the politics of protection, with insightful analyses on the securitization of cyberspace by the US (Bendrath et al. 2010, p.57), the challenges of complexity in theorising security in the digital age (Dunn Cavelty 2010, p.85), as well as liberal institutionalist approaches to a global information assurance regime (Valeri 2010, p.132) and an eclectic approach utilising the literature on international cooperation, regulation and policy diffusion (Hosein and Eriksson 2010, p.158). Such work is, of course, germane to the task in this book, which is to characterise and understand the EU's evolving ecosystem of cybersecurity. Indeed it is relevant in the sense that it reminds us of the complexity in analysing the politics of cybersecurity. Moreover, it demonstrates the need for an approach that does not neglect context, change and practice – both in terms of characterising the emergent ecosystem in the EU, and in identifying complex patterns of continuity and change in relation to how a resilient cybersecurity governance system for the EU is framed, constructed and practiced (see Christou and Croft 2012) by the plethora of actors involved in the European (and global) space.

Dunn Cavelty (2007, 2008a) approaches the issue of cybersecurity from a 'security studies' perspective, noting, as with Eriksson and Giacomello (2010), the lack of application of IR theory to the issue. Dunn Cavelty takes what she labels a semi-constructivist perspective, utilising the Copenhagen School focus on speech acts, and complementing this with framing and agenda-setting theory. Her approach has several advantages in analysing cybersecurity – and sits in the 'thin' constructivist school of thought – where there is recognition of the socially constructed nature of cyber threats, but where 'intentions and purposes are understood to be embodied within the objectified or institutionalised structures of thought and practice' (2008, p.7). Her emphasis then is not simply on speech as a discursive act, but also on how perceptions of actors can impact on and influence practice and action. The approach taken by Dunn Cavelty leads to a research agenda that focuses on how cybersecurity issues are constructed as a threat and placed on the agenda – and the subsequent post-securitisation phase in terms of the measures that are put in place to address cyber threats. Cavelty's main findings are interesting and obviously have implications for governing cybersecurity in the EU – in particular with regard to justifying and maintaining certain types or modes of (exceptional) governance in the

absence of what might be deemed real or tangible threats. However, whilst such an approach is intellectually useful in providing context with regard to historical framing and change, it does not explicitly relate construction of policy to governance forms (see Christou et al. 2010; Christou and Croft 2012). More specifically, it misses the detail of evolving governance arrangements[2] in the context of the security as resilience that is emerging. So whilst context will not be neglected in this book on the EU's policy and practice in cybersecurity, the key questions will not simply focus on how cybersecurity was securitised or not, but also on how practice is shaping the logic and nature of resilience within the evolving ecosystem of cybersecurity governance.

Another way in which cybersecurity has been approached conceptually is through the notion of cyber power. In an attempt to demonstrate the types of behaviour, instruments and resources that can be used in the cyber world by state and non-state actors alike, Joseph Nye Jr (2010) defines cyber power, in its wider sense, as 'the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power' (2010, p.4). He further differentiates between physical and information instruments, and hard and soft power in cyberspace, and gives examples of how they can be used inside (intra cyberspace power) and outside (extra cyberspace power) (Joseph Nye Jr 2010, p.5).

The relevance of the concept of cyber power is its links to modes of governance available to actors in cyberspace and importantly, the type of resilience and thus cybersecurity that an actor or state wishes to achieve. Whist Nye Jr shows how hard and soft power are connected to the three faces of power (Ibid., p.7), such power is also reflective of how actors, including the EU, can regulate and govern in relation to information assurance and threats to critical information infrastructure. Furthermore, it demonstrates the power resources of the actors involved in any cybersecurity ecosystem, with Nye Jr arguing that although within cyberspace there has been a narrowing of the gap between state and non-state actors across certain dimensions, this has not meant equalisation across the board; in other words, governments remain the strongest actors in resource terms, even though networks become more important as a tool of governance. He thus posits that governments have at their disposal varied forms of cyber power solutions, hard and soft, for different cyber threats (economic espionage, crime, cyber war and cyber terrorism), both inward and outward looking in nature, each affected by space and time. Whilst he argues within this frame that various offensive and defensive strategies are available to governments given their power

capabilities, he also demonstrates the difficulty of international cooperation on regulation or 'norms of behaviour' in areas such as cybercrime or cyber espionage (Ibid., p.18).

Betz and Stevens (2011), much like Nye Jr (2010), focus on state strategy and cyber power, although they by no means exclude the role of non-state actors in cyberspace. Indeed, they understand cyber power as 'the variety of powers that circulate in cyberspace and which shape the experiences of those who act in and through cyberspace' (Betz and Stevens 2011, p.44). Moreover, they recognise that in a socially complex 'networked society' driven by technological innovation the power of non-state actors increases substantively; and they also recognise the fluidity of cyberspace, which is made up of multiple actors and constantly in flux (Ibid., p. 38). They argue that much of the fear emanating from states is due to the proliferation of the many actors in cyberspace that seek to exploit the opportunities offered to them in order to achieve their own objectives. In their words, 'These range from individual citizens to civil society organisations and commercial enterprises, from terrorist and insurgents to branches of state power . . . to multilateral global institutions and media conglomerates, from individual nodes to whole networks, and non-humans in the form of hardware and software . . . ' (Ibid., p.38–39).

In recognising the complexity of power in cyberspace, they seek to extend the conception of cyber power, identifying four distinct forms: 1. Coercive/Compulsory, which is the use of direct coercion by one cyberspace actor in an attempt to modify the behaviour and conditions of existence of another and can be exerted by state and non-state actors and found in interactions between the state and non-state actors and between non-state actors; 2. Institutional, which is the indirect control of a cyberspace actor by another, principally through the mediation of formal and informal institutions and can be utilised by governmental (including sub-state) and non-governmental actors; 3. Structural, which focuses on how power works to maintain the structures in which all actors are located and which permit or constrain the actions they may take with respect to others that they are connected with directly; 4. Productive, which refers to the constitution of social subjects through discourse mediated by and enacted in cyberspace, and which defines the fields of possibility that facilitate and constrain action (that is, the discursive construction of threat actors in cyberspace to legitimise action against them) (Betz and Stevens 2011, p.45–53). Of course in identifying such powers, they also recognise that they are interdependent. That is, cyber power is not a monolithic concept so that in investigating

instances of power in cyberspace, a holistic approach must be taken that allows for the possibility that all four forms might be present in any given scenario (Betz and Stevens 2011, p.52–53).

Klimburg (2011a) also draws on the notion of cyber power. The dimensions of cyber power that Klimburg outlines as important are: coordination of operational and policy aspects across governmental structures; coherency of policy through international alliances and legal frameworks; and, cooperation of non-state cyber actors. He argues, contrary to Nye Jr, that of these dimensions the third is the most significant given the nature of the Internet and cyberspace; the majority of control comes from business and civil society and the capability of the state is limited to indirect rather than direct influence. In this context, Klimburg, drawing from the Integrated Capability Model (see Klimburg and Tiirmaa-Klaar 2011, p.11), posits the need for an integrated approach to cybersecurity, whereby, in his view, 'the non-state sector must be induced to cooperate with government', going on to argue that 'the most important dimension of cyber power is thus the ability to motivate and attract one's own citizens, an inward-focused soft-power approach that is fundamental for creating a "whole of nation" cyber capability' (2011, p.43). He points out that the US has been slow to realise how important an integrated approach to cyber power is, and argues that Russia and China both 'have highly capable and highly visible non-state cyber capabilities that interact with their governments' (Ibid., p.43–44). What he is effectively advocating is a public-private partnership model, which is guided by common goals and objectives. Whilst providing some examples of involved state and non-sate actors in China, Russia and the US (as well as the UK and EU) he does not elaborate conceptually on the nature of such partnerships beyond the need to build mutual trust, or indeed what the mechanics of any such partnerships would look like for cybersecurity in the EU and Europe more broadly. Suffice to say that the Chinese and Russian models of co-option, coercion and criminal network collaboration, are not governance examples that would fit with the EU's norms and values for cybersecurity and Internet governance more broadly (EU Principles and Guidelines 2011), even though the overarching normative notion of partnership and an 'integrated' approach is desirable.

Klimburg and Tiirmaa-Klaar (2011) apply the concept of cyber power as defined in the above three dimensions in a report written for the European Parliament. Here the central conclusions are that whilst the EU's cybersecurity policies in the areas of cybercrime and Critical Information Infrastructure Protection (CIIP) are contributing to an overall

resilience within the EU (resilience is not defined in any way), its cyber warfare capabilities remain underdeveloped through its CSDP. More fundamentally, and in terms of the dimensions of cyber power, the EU's own institutional systems are found wanting in terms of vulnerability to cyber-attack. Although the establishment of an EU Computer Emergency Response Team (CERT) has helped to remedy this somewhat, inadequate implementation of Information assurance measures have left the EU institutions open to attack, with poor information-sharing among officials involved in cybersecurity policy. Furthermore, in terms of coordination and indeed coherence, there is no single body responsible for EU cybersecurity policy, and neither does a single policy exist (which is still the case even though there is a Cybersecurity Strategy). On the international stage, it is argued that the EU's activity could be significantly improved on issues of cybersecurity, in particular in institutions such as the Internet Corporation for Assigned Names and Numbers (Ibid., p.36).

Internally, it is argued that within the post-Lisbon CSDP there is little activity in creating an integrated cybersecurity policy for the EU. More precisely there is 'no concept of projecting "hard" or "soft" power via an integrated approach to cyber power, and therefore for helping to define international cybersecurity around the core values of the Union' (Ibid., p.37). On the positive side, it is argued that the EU's research programme funding on cybersecurity has contributed greatly to supporting resilience, and the European Commission has been critical in driving forward the agenda for developing cybersecurity policy horizontally and vertically across the member states (in particular weaker members).

Beyond this, the study finds – quite significantly in the context of the third dimension of cyber power outlined by Klimburg (2011a), cooperation with non-state cyber actors (civil society and the private sector) – that the EU's engagement is underdeveloped. It is argued that for 'resilience' to evolve, the EU must improve its efforts to consult with civil society (volunteer technical actors that work on open software, for instance); which historically the Commission has been open to doing. The EU must also do the same with regard to private actors. Although initiatives to collaborate and share information do exist through, for example, the European Public Private Partnership for Resilience (EP3R) (replaced by the Network and Information Security Public Private Platform – see Chapter 6) the report suggests that a truly European approach for sharing information on cyber-attacks is far from constituted.

The cyber power literature obviously raises interesting issues for the EU's emergent ecosystem of cybersecurity governance and the EU's

approach to cybersecurity. The EU is not a traditional state *per se*, but rather has its own particular institutional make-up – and mixture of supranational and intergovernmental mandates with varying member state security logics when it comes to cyber defence and offence – in the case of cybersecurity. Thus, it is argued, that whilst an integrated approach is necessary for the EU to remain true to the values and principles that it espouses for the Internet and to achieve a sustainable, adaptable and flexible resilience, it should focus on developing its soft power capabilities – influencing the structural and (re)constructing the institutional – rather than any form of hard coercive power.

Hard power and the development of offensive capabilities, in any sense, is difficult if not impossible for the EU given the sensitivity this holds within its member states, but neither is it desirable, it can be argued, if the national security logic that drives it undermines the rights of individuals, excludes key stakeholders, erodes trust and potentially creates greater vulnerabilities in the cyberspace ecosystem (Dunn Cavelty 2013, 2014; Christou 2014). The structural element is clearly important in relation to the context within which the EU is constructing its strategy and influencing others within a multipolar networked world, and the constraints and opportunities that exist in terms of implementing such a strategy, which is inevitably underpinned by the notion of balance between rights and security. The institutional aspect is also significant for the EU – both in terms of its interactions with the relevant global institutions and private organisations concerned with cybersecurity, and the role of its own institutions and in particular agencies, such as ENISA and the European Cybercrime Centre (EC3) in constructing security as resilience in cyberspace. A question that the cyber power approach does leave open, and which this work intends to fill, is that of what sort of governance approaches and associated instruments and platforms can best facilitate the creation of the conditions required for an effective security as resilience to emerge in Europe.

In this sense, Mueller's (2010) work is informative as he uses governance as the central guiding theme in his analysis of the global politics of the Internet. Indeed, although Mueller does not simply focus on issues of cybersecurity, the conceptual question he poses is an interesting one: Where can we locate issues and policy arenas within Internet governance, such as cybersecurity, privacy, etc., given the reality of both peer production (non-hierarchical governance) or transnational networks, and government or state control (hierarchical governance) in Internet governance more broadly? In this context he seeks to theorise networked governance, and argues that it can only be useful in

analysing Internet governance if it is used precisely – as a theory of organizational forms, in which we can distinguish between: 'the clustering of political actors in unbounded networks of influence around governance institutions, and networks as a bounded consciously constructed type of organization' (2010, p.51). Following from this he proposes four ways in which networked relations can produce institutional change: by formalizing and institutionalizing the network relations themselves; by states' attempts to impose hierarchical regulation upon networked forms; by states' utilization and adoption of networked forms; by challenging the polity through realigning and expanding the associative clusters around governance institutions.

When testing these propositions in relation to cybersecurity using spamming and phishing as cases, he argues that although much legislation has been passed in the US and EU in the area of cybercrime, as well as international law such as the Council of Europe's 'Convention on Cybercrime', such 'residues of hierarchy are becoming entirely dependent upon the networked relations of peer production to have any effect . . . the agents of hierarchy . . . must participate in and become integrated into the looser trans-jurisdictional, multi-stakeholder networks of operators' (Ibid., p.173). His conclusion is that despite a certain securitisation by the US government of the cybersecurity issue,[3] and the call for harder forms of 'cyber power' to combat the impending threats from cyberspace, such modes of power cannot exist independently of softer, existing and emerging forms of peer produced and transnational modes. Indeed, what is also interesting about his argument more broadly, (which is consistent with the argument made above on hard power), is that implicit in it is the need to preserve liberty and openness in order to ensure security (Ibid., p.180). The securitisation of cyberspace, in other words, whilst ratcheting up resources and extraordinary means to deal with threats, can also legitimise the use of such tactics for cyber terrorists and criminals. This in turn can result in greater cyber insecurity rather than security as resilience.

Mueller's approach then, is salient for an analysis of the EU cybersecurity regime. The EU ecosystem for cybersecurity is formative and interesting questions emanate from the nature of the interaction between EU agents, and those networks and actors involved in the peer production of cybersecurity globally and in Europe. Moreover, taking Mueller's analysis further, important questions about the nature of the emergent logics of resilience – and of coordination, collaboration and trust – need to be answered if the EU is going to make progress in constructing a common approach to cybersecurity issues, in particular in

relation to public-private partnerships. Beyond this, we need to ask questions not just of the institutions and networks of governance, but which particular modes of governance are prevalent across cybersecurity issues, and under what conditions, political, legal and technological, they can sustain adaptable resilient ecosystems.

Understanding the European Union in cybersecurity

Ecosystems and resilience

Having reviewed the dominant literature on cybersecurity, this section will aim to elaborate on the central conceptual argument and framework through problematizing resilience and security governance. To reiterate, the argument here is that such literatures are very much relevant to understanding the EU's evolving cybersecurity strategy and approach – concepts of cyber power, security logics and governance have important implications for the type of resilience that can be achieved. We need therefore a more in-depth exploration of resilience and its relationship to security governance in order to construct a comprehensive frame for understanding what is evolving at the EU level and the conditions necessary for the EU to develop an effective security as resilience approach, underpinned by instruments, tools and mechanisms that allow the EU to achieve a more secure cyberspace.

Fusing the concepts of resilience and security governance in order to construct and establish a security as resilience approach, will allow the characterisation of emerging security governance practice in EU cybersecurity and more importantly, how this equates to achieving certain types of resilience. Whilst there will be a predominant focus on output in such an assessment given the formative nature of the EU cybersecurity ecosystem (activities such as issuing reports, producing research, producing policy initiatives, creating new mechanisms, platforms and institutions and so on), it will not exclude assessment of outcome (changing behaviour) and impact (changes of target indicators such as a reduction in cybercrime) (see Szilecki et al. 2011, p.716) where practical and feasible.

To elaborate further, a governance solution that has been prominently projected in many policy reports and indeed activities of global and regional institutions involved in cybersecurity and cybercrime has been that of public-private partnership (PPP; see ENISA 2011d). The EU established the EP3R and its successor the Network and Information Security Platform (NISP – see Chapter 6) for this very purpose, and PPPs form one of the four central pillars for deliberation within the EU–US Working

Group on cybersecurity and cybercrime. However, whilst cyber power approaches posit coordination and cooperation as important between different actors, they do not go on to specify, beyond building mutual trust or collaboration, the types of partnership possible or desirable or what might constitute effective partnership. Furthermore, resilience, whilst appearing as a leading mantra in developing cybersecurity and information assurance policy, is not problematized in the academic approaches reviewed in the section above.[4] There is no conceptualisation of the logics of security governance and resilience that should evolve within the EU dimension, and what they mean for preparedness, protection, detection, response and recovery. Indeed such problematization and conceptualisation has been more prominent in the work of EU policy agencies such as ENISA, as well as international organisations such as the Organisation for Economic Cooperation and Development (OECD) and the United Nations (Economic and Social Council and the International Telecommunications Union).

The EU agency ENISA has used the language of natural ecosystem with reference to Internet interconnection, drawing on engineering and systems biology and defining resilience as 'the ability to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation' (ENISA 2011c, p.10). The starting point in this book, drawing from the literature on resilience, is to utilise the ecological metaphor in order to understand cyberspace as an evolving 'ecosystem' that has the potential to self-regulate (Holling 1973; Walker and Cooper 2011). This conception of ecology, 'suggests that inter-connected and inter-related ecosystems have the capacity to change and adapt in relation to shocks' (Brassett and Vaughan-Williams 2015). Resilience within ecologies has been explored through a critical-theoretical literature (Lentzos and Rose 2009; Walker and Cooper 2011; Brassett and Vaughan-Williams 2015), which seeks to deconstruct and question how and why resilience is posited as a solution to certain problems, and a problem-solving, conceptual literature that seeks to deepen our understanding of types and logics of resilience. The intention here is not to ignore the critical[5] – that is, questions on the compatibility of certain logics of resilience and governance, for example flexibility and adaptability vs efficiency. At the same time, however, it primarily seeks to engage with existing typologies of resilience in order to first, elaborate on the security governance logics that might underpin them and second, to provide an idea of the extent to which they can produce certain resilience outcomes in EU cybersecurity. This is not to assume that any such typologies are fixed, complete or not contestable within the

cyber ecosystem. Rather the aim is to provide a fluid menu of conceptual markers, against which an assessment can be made in relation to change and output.

The focus on cyberspace as a natural ecosystem, of course, is not incompatible with considerations of the 'politics of resilience' in cybersecurity; indeed, the ecology metaphor has evolved – both in terms of the natural and social sciences – as a way of understanding resilience within ecology or ecologies of resilience (Holling 1973). More specifically, the concept of ecological resilience developed as an alternative to the notion of engineering resilience, an abstract variable associated with mathematical ecology which denoted 'the time (t) it takes a system to return to a stable maximum (or equilibrium position) after a disturbance. The return is simply assumed, and the equilibrium state is taken as equivalent to long-term persistence' (Walker and Cooper 2011, p.146). For Holling, such a managerial approach to resilience was problematic, not least because it was premised on the notion of predictive knowledge, and the assumption that future events are expected. Rather than providing a definition that was mathematical and quantitative (Grimm and Calabrese 2011, p.7), Holling sought to put forth a more complex notion of resilience that went beyond stability and returning to equilibrium, and which emphasised the persistence of relationships within an ecosystem. Importantly, Holling was critical of the management approach's assumption that future events are expected, or can be predicted, arguing instead that 'the resilience framework . . . does not require a precise capacity to predict the future, but only a qualitative capacity to devise systems that can absorb and accommodate future events in whatever unexpected form they may take' (Holling 1973, p.21).

Such a conception of resilience and Holling's later contributions to adaptive ecosystem management not only earned him a wide following but led, through consensus and collaboration, to the formation of the Resilience Alliance and many definitions of ecological resilience premised on his ideas (see Brassett and Vaughan Williams 2015). Indeed, the concept of ecological resilience was extended to take into account not just the robustness and persistence of systems, but also social ecological resilience, which focused on adaptive capacity, transformability, learning and innovation (Brand and Jax 2007; see also De Bruijne et al. 2010, p.19). What is important and salient about these approaches to resilience, and indeed what they have in common is their emphasis on the concept of ecology as a set of relationships, and as system that is contingent and precarious. This is critical in analysing cybersecurity where

the technical or scientific and social or political layers are inexorably linked within an ecosystem and where the relationship between the layers must be mutually reinforcing in order to achieve an adaptive and effective resilience.

Furthermore there is a clear link between the broad conception of resilience and the assumptions of complex systems theory, which emphasises the properties of open and adaptive systems, non-linear logics, limited (un)predictability and significant limits to knowledge and progress due to uncertainty (Kavalski 2009, p.532). It also clearly interconnects with the metaphor of global fluid, defined as 'partially structured by . . . the network of machines, technologies, organizations, texts and actors that constitute interconnected nodes along which flows [of capital, ideas, social energies, etc] can be relayed' (Betz and Stevens 2012, p.38). Importantly, 'these fluids do not respect established morphological and social boundaries and "may escape, rather like white blood corpuscles, through the wall into surrounding matter and effect unpredictable consequences upon that matter". This non-linearity means that a global fluid like cyberspace cannot simply be dismantled . . . nor its behaviour readily predicted . . . Neither a wholly social, nor a narrowly mechanistic view of cyberspace sufficiently captures its operations and experiences . . . At all times, cyberspace is an assemblage of multiple actors whose relations are never permanently captured' (Betz and Stevens 2011, p.38).

What such notions point to then, which is important for the framing of this work and the argument made in the book, is a more complex conceptualisation of security governance – or *security as resilience* (Kavalski 2009, p.532) – which not only seeks to delineate governance mechanisms suitable for cybersecurity, but rather, provides an understanding of the mechanisms, relationships, characteristics and processes that can lead to effective resilience – in this case within the EU cybersecurity domain. In this context conceptions of security governance are intimately linked with types of resilience, and there is an attempt to move away from notions of security governance as *security of control* which focus simply on change within and between systems (Webber et al. 2004, Webber 2007; Kirchner and Sperling 2007a, 2007b; Hallenberg et al. 2009), thus excluding the possibility of the emergence of 'ecosystem' resilience (De Bruijne et al. 2010); that is, resilience which allows for the possibility of a change to systems and the emergence of new adaptable regime(s). Such resilience is proactive rather than reactive, accepting rather than resisting the inevitability of change and the creation of a system 'that is capable of adapting to new conditions and

imperatives'. Reactive resilience, on the other hand, focuses on strengthening the status quo and resisting change in order to achieve stability and constancy within an ecosystem (Handmer and Dovers 1996, p.494).

Such typologies then, even though representing extremes on the resilience spectrum, are a useful starting point for facilitating our understanding of the emergent ecosystem of resilient cybersecurity governance within the EU. They can provide us with a range of potential responses to different types of security challenges, risks and attacks in cyberspace (small-scale, medium and major), and importantly, they can help us to characterise how the ecosystem within the EU is evolving, and what the implications are in terms of actors, processes and mechanisms, as well as relationships and institutional structures. It also allows the construction of propositions and a framework that can be tested in order to provide insight on the direction, strengths and weaknesses of practice. To this end, Handmer and Dovers (1996) provide a threefold classification of resilience that can be extended for achieving the aims of this book: Resistance and Maintenance (Type 1); Change at the Margins (Type 2); Openness and Adaptability (Type 3). Indeed by utilising such a frame and extending the security and governance underpinnings, a greater sense of what is required to achieve the flexibility and adaptability required (Type 3 resilience, see below) – technical and political – to cope with unexpected threats will emerge. By providing benchmarks against which the existing and emerging features of the EU cybersecurity ecosystem can be understood, the approach being taken can be comprehensively and critically assessed with regard to potential outputs.

The typologies of resilience provided by Handmer and Dovers (1996) are intimately connected with the interpretations of resilience already alluded to above. They also need to be adapted and elaborated upon for the purposes of analysing cybersecurity in the EU, given that Handmer and Dovers (1996, p.495) discuss such typologies at the generic level. Furthermore, any such typology also needs to be extended to add further nuance to the possible security governance mechanisms and processes at play within each type, in particular with regard to the relationship between public and private actors in the form of partnerships, which have been, alongside anticipatory risk management, the dominant approaches to providing resilience within Europe (ENISA 2011d, p.25; see also Schoon 2010).

Type 1 resilience is characterised by sovereignty, hierarchical governance, state control of resource and information, resistance to change and an emphasis on maintaining the status quo through

resource investment and appeals to ignorance. That is, in the case of cybersecurity, those actors (state or non-state) with power might argue that the threat is exaggerated and appeal for more evidence of real threat. Furthermore, because of its emphasis on stability and certainty, such resilience is incapable of responding and adapting to the unpredictable (that is, new circumstances). This lack of flexibility though can have its positives in terms of maintaining optimum capacity and indeed existing power structures in the short term, especially for those that do not wish to concede power. However, the question remains as to whether this type of resilience is sustainable in the medium to long term. It might be argued that such resilience may result in sustainable security governance; it is stable and able to take the strain, and may result in a completely new order if it does collapse. On the other hand, this might well cause irreversible damage with many social, economic and political consequences, and in the worst case scenario, could cause the complete collapse of an ecosystem, without the ability to rebuild (Handmer and Dovers 1996, p.495–499).

Type 2 resilience typifies the approach usually taken to manage risk (which is underpinned by traditional linear risk assessment). There is recognition that a problem exists and that change is needed for the system to become more sustainable. It is a problem-solving approach that is characterised by discussion and reform that leads not to transformability, but policy changes that effect outcomes at the margins. Such an approach addresses the symptoms of the problem rather than its causes. The consequence of this is that there are no wholesale changes with regard to new legal and technical protocols and standards or global codes and rules of conduct on the Internet that might lead to *corrective* (instrumental) rather than *antidotal* (transformative) cultural adaptation by the key actors in cyberspace (Boyden 1987, p.24). Whilst it can be argued that such a problem-solving approach results in the identification of problems and policy measures to resolve them; they are usually driven by short-term efficiency logics and linear methods and therefore any minor change that does occur has minimal impact on the cause.

Moreover, such minor changes can lead to the impression that something is being done by the institutions and actors involved within the ecosystem; in particular as the agenda is still state controlled (as are power structures) even though there is an increase in participative mechanisms. At the same time such minor changes might actually act as a delay to any major, innovative, transformative changes that are needed to sustain resilience, in particular in more complex ecosystems. Obviously such an approach is bounded by embedded political structures,

with domestic constituents interested in the here and now, rather than the longer term. This also makes it much easier to sell the incremental approach as the only real and palatable option. Another issue if substantive change does occur in Type 2 resilience is that of who benefits from such change. Within cybersecurity this is a very important question given that any given cybersecurity attack or cybercrime can affect not just public and private sector elites, but also civil society and individual citizens. In this context, the question of inclusiveness is important if transformative ideas are not simply going to be subsumed and watered down by political elites, to their benefit. Type 2 resilience is perhaps the most common response to threat and risk; it is portrayed as pragmatic and balanced and perceived to be the most palatable, economically and politically. Whilst this no doubt is beneficial in the short term however, this efficiency drive approach focused on the market and individual choice, sits in potential contradiction to a secure, transformative, long-term resilience solution (Handmer and Dovers 1996, p.499–501). This tension between efficiency and medium to long term resilience is highly problematic for creating a more sustainable and consistent resilience (ENISA 2011c, p.13).

Type 3 resilience is characterised by flexibility and the ability and preparedness to adopt 'new basic operating assumptions and institutional structures' (Handmer and Dovers 1996, p.502) and in governance terms is more likely to lead to major change in power relationships, participation and inclusiveness (this being self-organised and non-hierarchical). Rather than providing resistance to uncertainty as in Type 1, the actors involved would embrace new ideas and embark on major changes in order to create an ecosystem that can reduce vulnerability to threat. An ecosystem would be created, in the case of cybersecurity that is diverse and has spare capacity, with the underpinning assumption of efficiency abandoned in favour of complexity in operating assumptions in order to avoid single points of threat and failure. Such transformative change is not easily achieved, operationally, structurally or culturally, given that it involves new ways of doing things, and has implications on vested interests and on the relationships between different actors in cyberspace. This is even more complex in cyberspace given that not all 'state' (or non-state for that matter) actors have the same approach to cybersecurity, and that within cyberspace many tensions exists between advocates of liberty as security and conversely, more security (or securitisation) for the preservation of liberty (often states). Moreover, in areas such as Critical Information Infrastructure Protection (CIIP) and

the security of domain names, where private interests and actors dominate or are influential in implementing new technologies or systems, and where there is an economic or cost logic to doing so, it is difficult to incentivise truly transformative ideas.

Whilst there are many inhibitors to real change then, Type 3 resilience does implicitly assume that, and its success relies on this, coalitions of actors working together in partnership to construct new flexible and adaptive institutions and operating procedures, set the agenda and implement policies. In this way this type of resilience is seen as the most likely to deal not just with the symptoms, but also the underlying causes of cybersecurity problems, at individual and institutional levels. Type 3 resilience might also have negative effects such as increased costs and inefficiencies resulting from diversity; but such diversity and the increased complexity that this brings with it, would ensure that any ecosystem is able to adapt and change through a choice of options and directions. Similarly, due to its complexity and the inability to anticipate and predict potential risks and threats, maladaptive changes are possible that have negative consequences in the short term. Indeed, and as Wildavsky (1988) has argued, 'decision-makers will have to increasingly rely on risk-tolerant, flexible decision-making strategies that allow for trial-and-error and learning as society's capacity to anticipate risks and dangers fails to keep up with the growing complexity and dynamics of the world in which we live' (in De Bruijne et al. 2010, p.22). Moreover, this can be achieved by adapting a variety of strategies, which as well as the structural elasticity already alluded to, include high-performance relationships between the relevant stakeholders, and a culture of reliability and improvisation. Institutions and organisations must 'learn how to learn' if they want to enhance their capacity to adapt (Ibid., p.23), and unlike specific defences under the (traditional) anticipatory risk approach, this requires 'knowledge, communication, wealth and organizational capacity, and the resources that enable us to craft what we need, when we need it, even though we previously had no idea we would need it' (Wildavsky 1995, p.433).

Security and governance

What then, do these typologies provide for the task in hand: an assessment of the emergent resilient security governance ecosystem for cyberspace in the EU? As Dunn Cavelty (2013, p.6) notes, 'If resilience is a core concept, security does not refer to the absence of danger but rather the ability of a system . . . to reorganise to rebound from a potentially catastrophic event.' In this context, typologies of resilience

provide certain markers to allow us to understand some of the characteristics and relationships emerging in such an ecosystem – and most importantly – the type of resilience that is being constructed. Indeed it also allows us to sketch out the general conditions required for the emergence of highly effective security as resilience systems (see Box 2.1). This in turn, is important for being able to judge what is actually emerging in terms of specific 'governance' modes, methods, mechanisms and actors. This is where the resilience literature falls short and where the broader governance and specific security governance literature can be fruitful, in the elaboration of the emergent type of security logics and governance in the EU's cybersecurity ecosystem, across different dimensions.

Box 2.1 Conditions for achieving effective security as resilience in cyberspace

- Ability (including resource and mandate) and preparedness to adopt new basic operating assumptions and institutional structures
- Assumption of efficiency abandoned in favour of complexity in governance logics in order to avoid single points of threat and failure
- Coalitions of actors working together in 'partnerships' based on trust to share information, construct new flexible and adaptive institutions and operating procedures, set the agenda and construct/implement policies
- Convergence amongst stakeholders on a 'common' understanding, logic(s), 'norms', laws and standards of security as resilience
- Evolution of a culture of cybersecurity at all levels and layers (technical, legal, policy) among all stakeholders (awareness, education, learning and so on)
- An integrated approach (coherence and consistency across layers, levels, actors)

However, the problem with the traditional security governance approach is that it does not develop governance in the context of complexity (Schneider 2012, p.130) and thus offers little insight into the

meta-governance[6] (Cavelty 2008b; Shore et al. 2011) of public and private actor relationships. Thus we need to elaborate on the specifics of what partnership or participation actually means in relation to the actors involved, or indeed the modes of governance through which transformative resilient security can be achieved (hierarchical, non-hierarchical or hard/soft); which is important given the multitude of stakeholders in cyberspace, and more importantly, given that public-private partnerships have been identified as one of the key governance mechanisms for addressing issues of cybersecurity given its global nature (Non-paper, On the Establishment of EP3R, 23 June 2010; ENISA 2011d). Note the purpose here is not to be prescriptive about which type or mix of meta-governance is best suited to achieving the conditions for effective security as resilience (Type 3). Even though Type 3 resilience is underpinned by certain overarching features it will be an open empirical question for assessment with regards to the evolving EU cybersecurity ecosystem. Indeed much debate still exists on what the optimal public-private (mandatory-voluntary) balance should be for highly resilient systems to emerge (Dunn Cavelty and Prior 2013) within the EU and internationally.

It is also important, for this work, to elaborate further on evolving partnerships between the public and private sector, and what this means for cybersecurity in terms of resilience in the EU. This entails moving beyond macro 'systems' of governance as alluded to in the traditional security governance literature – regional, global, Westphalian, post-Westphalian, etc. (Hallenberg 2009, p.8), to specifying aspects or characteristics of forms and potentially functions. The point here is not to provide an exhaustive list of types, but to outline certain approaches towards, as well as shared characteristics and features of partnerships to aid us in our understanding and possible elaboration, through assessment of practice, of what is emerging within the EU cybersecurity ecosystem specifically. To this end, Shore et al. (2011, p.6–7) provide an outline of three broad public-private collaboration approaches that are useful for this work. The first is the meta-governance of identities or market forces. This approach provides for: a clear rationale for private sector involvement; is clear on which private actors would be responsible for delivering outcomes; is characterised by clearly defined goals and tasks and the cultivation of collaborative partnerships between government and industry. A potential criticism of this type of self-regulatory, private industry-led approach is that of potential negative outcomes – in particular with regards to cybersecurity if the guiding logic is that of the market and thus profit (likely to be exacerbated in times of economic crisis).

The second is that of hands-off meta-governance, which is characterised by indirectly influencing partnerships through changing the environment. This can be done, for example, through: coordinative arrangements (platforms, networks, advisory boards, ad hoc mechanisms); facilitation, through supporting partnership and helping them to work efficiently through, for example, frameworks for interaction or granting exemptions from law that impedes private collaboration; and finally, stimulation, which can take the form of economic or social incentive plans to increase private participation and can be voluntary or incentivised (for example, giving advantage to suppliers who satisfy partnership obligations).

The third is that of hands-on meta-governance characterised by more direct influence from the public sector. Thus influence might take the form of public sector participation through facilitation and administration of collaborative networks; monitoring and influencing private sector activity through legal and non-legal mechanisms; lowering costs; and neutralising conflict between private actors. A potential criticism of such a public-led, ultimately top-down approach is the potential conflict of interest that can result between public actors as regulators and perhaps quite saliently in cybersecurity, the lack of trust by industry if public intentions, activities and outcomes are perceived to be negative. These three broad types then can facilitate the location of the EU's evolving approach to resilient cybersecurity governance, capturing variations within, between and potentially beyond them.

Further to this and in line with the concept of *security as resilience* rather than *security of control*, the EU's evolving ecosystem and the organisational forms within it, are considered as fluid, dynamic and changeable. To this end forms of collaboration and partnership within the EU ecosystem can be captured at different levels and dimensions of governmentality (national, transnational, multilateral and so on) which at different points in time can potentially take the form of long-term community, an organisation/institution with varying functions and responsibilities, well-defined working groups, loose (issue) or tightly coupled (policy) networks, and response and activity groups (ENISA 2011d, p.28). In turn, such forms can be public-private, private-private or multi-stakeholder and formal as well as informal. Any such forms are interconnected with governance (see Flyverbom 2011, p.66–67) and meta-governance (Shore et al. 2011, p.6) and in turn, security as resilience, and they are neither fixed nor stable. Indeed, we can only make sense of form, function and scope if we understand the why and how of interaction among actors. This can then also give us further

insight into the potential barriers to performing resilient security governance within the evolving EU ecosystem, and indeed the extent to which the EU can actually move to a highly resilient (Type 3) ecosystem.

As has already been alluded to above, the focus in this book is on *security as resilience* rather than the *security of control*. The latter is very much connected to the traditional literature on security governance – in other words, it is underpinned by assumptions of predictability and consistency – key features of Type 1 resilience as well as traditional linear methods of risk and threat assessment (Type 2 resilience). It would thus seem that there is a contradiction between adaptive Type 3 resilience and traditional security governance that cannot be reconciled (see Kavalski 2009, p.531–532). However, whilst this might be the case in terms of 'approach' at the level of epistemology, where it is useful, is in its emphasis on how the governance of security has become more complex within the context of globalisation and regionalisation in terms of the actors, processes and mechanisms at play. Indeed it is underpinned by the assumptions that the state is no longer the single most important provider of international security, and that the responsibility for security in a globalised world is dispersed among state and non-state actors. In addition, security structures or a coalition's fluidity and flexibility represent a distinctive characteristic of security governance, so that security coordination takes on different shapes (Krahmann 2003, p.5). Security governance thus, is described as 'the coordinated management and regulation of issues by multiple and separate authorities, interventions by both public and private actors, formal and informal arrangements, in turn structured by discourse and norms, and purposefully directed towards particular policy outcomes' (Webber et al. 2004, p.4).

Of particular importance is the working and coordinating mechanisms of security governance within and across issue areas. In this regard, co-ordination, management and regulation are the three components of governance and also the three tools used to empirically test it. Specifically: Co-ordination concerns the way in which actors interact and who, among them, leads policymaking, implementation and controls the process; Management relates to risk assessment duties, monitoring, negotiations, mediations and resource allocation; Regulation is conceived as the policy result: its intended objective, its fostering motivation, its effective impact and the institutional setting created (Kirchner 2007b, p.24).

What is relevant to building and adding to the governance dimension of the resilience typologies above is security governance not simply as heuristic device (Kirchner and Sperling 2007b, p.18), but as a theory of

emerging (collaborative) networks within the cybersecurity ecosystem (Krahman 2003). In this sense the security governance approach can facilitate our understanding of the interactions among different actors, and if extended, the nature of these interactions in terms of the type of resilient cybersecurity ecosystem that is emerging in the EU. Security governance classifies cybersecurity under the category of 'protection': with the main governance tool identified for combating it, institution-building – be it of a formal or informal nature. It also seeks to identify the ideational underpinnings of the relations between actors – whether structured by norms or formal, legal regulations (Webber et al. 2004). What it does not do, however, is elaborate on forms and types of relationship emerging, why they are emerging, and what the potential tensions are between different actors within the cybersecurity ecosystem, whether in formal or informal settings.

This is particularly salient when discussing the practice of resilience in the emerging EU cybersecurity system as it allows the analyst to focus on and emphasise the politics of resilience in practice, through exploring why particular institutional forms (or norms) are constituted, the stake that particular actors have in the knowledge of security resilience (for instance, why they are involved), how actors interact, define policy objectives, and how both cultural as well as material factors hinder or enable the practice of security resilience and the constitution of any particular type of resilient security governance within an ecosystem. Exploring such aspects will not only provide insights into the issue of coherence within a particular environment and its settings, but also provide a platform for a more complex understanding of how actors within emerging institutional forms (formal and informal) understand resilience and subsequently how their knowledge defines their approach to the practice of resilient governance.

Conclusion: Security as resilience

This chapter has aimed to set out certain conceptual and theoretical markers that will facilitate the analysis of the EU evolving ecosystem of resilient security governance. Whilst there is an emerging literature on information assurance and cybersecurity, theoretically it has fallen short of providing a framework for analysing cybersecurity in terms of the type of *resilient* security governance that is emerging, or indeed the conditions that will enable the emergence of highly effective, resilient ecosystems. In addition, little in-depth, theoretically informed work exists on the EU's evolving cybersecurity ecosystem beyond the

application of cyber power.[7] What has been argued in this chapter is that incorporating and building on the existing literature on cybersecurity, a fusion of resilience and security governance can provide a valuable theoretical and practical insight into the EU's developing ecosystem of cybersecurity governance. Indeed, utilising the notion of *security as resilience* rather than *security of control*, and setting out general conditions for the construction of highly effective resilient systems (Box 2.1), facilitates an analysis that not only provides us with a sense of direction with regard to the EU approach in terms of the relationships it is constructing and constituting, but also provides a deeper understanding of why and how the EU is travelling in such a direction, in terms of the actors, networks and institutions involved, and the global ecosystem within which they are operating. Moreover, problematizing resilience and adding nuance to how it is defined and understood conceptually, as well as taking a critical approach to (cyber)security governance, will unveil the extent to which shared logic(s) of resilient security are emerging, and in turn, what this implies for the EU within the different spaces, levels, layers and dimensions that it must interact with in practice. Assessing the EU's evolving practice in cybersecurity in the proceeding chapters, will provide a basis for testing the construction of resilience practice in the EU and the governance constellations around these. In turn, it will provide the basis for theoretical and conceptual reflection with regards to security as resilience in cyberspace.

3
Cybersecurity in the Global Ecosystem

Introduction: The international context

According to Steve Purser of ENISA, 'International collaboration is essential. Security within national boundaries doesn't make sense. Everything is globally connected. A European approach doesn't make sense unless aligned to the approach of international partners' (SDA Report 2012). Thus the EU's construction of its cybersecurity ecosystem is embedded within, bounded by, and inexorably connected to the evolving global ecosystem of cybersecurity governance, and more broadly, Internet governance. The EU has emphasised in its Internal Security Strategy (November 2010) and the European Guidelines and Principles for Internet Resilience document (March 2011) the importance of working in partnership with global partners to address the civilian and military aspects of cybersecurity challenges. The global interconnectedness of the Internet ecosystem means that threats can emanate from any source around the world, which in turn requires solutions and policies that are borderless. The vulnerability of the Internet, and the interdependence between networks, information systems and individuals, makes it impossible for any single actor to assess and respond to cyber threats and risks. Moreover, national responses alone cannot be effective given the integration between electronic, economic and political networks across the globe, and in order to achieve this there must be a step-change in the coordination of approaches not only downwards, but also upward and outward to institutions, networks and actors, technical and political, that have a role to play in constructing security resilience within the many different aspects of cybersecurity.

This chapter will therefore provide an overview of the prominent global and regional institutions, networks and actors involved in the

security of resilience in cyberspace, and an assessment of the logics that are at play within the emerging ecosystem. Moreover it will assess how 'best practice' in cybersecurity, recommended or institutionalised in one way or another (through code, practice or law) at different levels, has been adopted by other actors, as a basis for understanding EU cybersecurity policy in the proceeding chapters. Whilst the EU has clearly been active across several fora, platforms and bilateral relationships, including the UN Group of Experts tasked to construct norms for cyberspace and the Organisation for Security and Cooperation which has designed confidence building measures, this chapter will only implicitly analyse the EU's role within different institutions, as this will be done more explicitly in relation to specific policy areas and the EU–US relationship in the chapters that follow. The ambition here is simply to provide a context, through conceptually informed assessment of what approaches (or debates) are emerging in the complex global Internet and cybersecurity landscape, in order to provide an understanding of the possible influences on the EU's emergent ecosystem of security governance in cybersecurity. The focus, for this purpose then, will be on the key actors and organisations involved in constructing a resilient governance ecosystem for cybersecurity[1] and in particular, on what sorts of logics of resilient governance are emerging. Indeed, a primary aim of the chapter, is to uncover the extent to which there is convergence or divergence in the approaches advocated by key global players, and what this, in turn, implies for the EU in its approach and emerging strategy on Internet security.

The chapter will be structured as follows. The first section will look at those institutions and fora that are active in discussing policy ideas and developing policy on Internet Governance (IG), which also have a stake in contributing to cybersecurity, such as: the Internet Corporation for Assigned Names and Numbers (ICANN) which primarily regulates the Domain Names and Numbering System; and the Internet Governance Forum (IGF), which was created from the International Telecommunications Union (ITU) led World Summit on the Information Society (WSIS). The IGF, which secured a second five year mandate from the UN in 2010, is not a traditional policymaking forum, but provides a platform where *all* stakeholders can come together to present proposals and different aspects of IG, including security. The second section will discuss multilateral fora, such as the G8, United Nations (ITU), North Atlantic Treaty Organisation (NATO), Organisation for Economic Cooperation and Development (OECD), and Organisation for Security and Cooperation in Europe (OSCE) that have been active in contributing

to the evolution of resilient governance for cyber threats, and which have produced a plethora of reports and recommendations on reducing cyber risk, developing cyber defence and deterrence, best practice in cybersecurity, and protecting critical infrastructures nationally and internationally. The final section will assess the security resilient logics emerging from the global landscape, and the implications of this for creating a flexible and adaptive ecosystem of governance for cybersecurity in Europe and beyond.

Internet governance and cybersecurity

ICANN

ICANN has responsibility for three critical Internet functions: the allocation of Internet Protocol number resources for individual computers and machines; their corresponding Domain Name Service names; and, the allocation of top-level domains (TLDs) to registries that assign identifiers to individual users and organisations globally. These three functions and how they evolve have important implications for Internet security, and the governance approach that underpins the Internet and its security. Important here, in the context of resilient security governance, is the challenge to self-regulation, which has been the dominant approach for managing Internet names and addresses since ICANN was established in 1998 as a not-for-profit, public benefit corporation, underpinned by California law. ICANN was founded on pre-existing technical organisations, with the purpose of exposing the Internet to public and private commerce (Klimburg 2011b, p.6). As the Internet has grown and evolved, so too has the role of ICANN, often through processes of internal reflection and review as well as external criticism and pressure. Moreover, as the issue of domain names has become more important, in a strategic sense, national governments as well as the EU have called for and, to a certain degree, secured a more active role in the formation of ICANN policy through the Government Advisory Council (GAC) (Christou and Simpson 2007, 2011). They have also exerted pressure on the US government with regard to the issue of accountability and influence – ICANN was originally contracted to the US Department of Commerce, with a very strong US influence on policy and its direction. Whilst this situation changed in 2009, under a new agreement, the Affirmation of Commitments (AoC), the issue of representation, influence and accountability are far from resolved. Furthermore, the strategic importance of domain names at national level has seen the strengthening of national registries to manage security and other issues

related to their country code top-level domain (ccTLD). These trends, alongside increasing technical developments have resulted in challenges for ICANN, in particular in the security realm, which it has sought to respond to. Perhaps not surprisingly, this has also had implications for the nature of resilient security governance evolving for domain names and numbers (European Parliament 2011), and more specifically, has undermined the self-regulatory principle that has underpinned Internet governance since its inception given the perceived 'public good' dimension attached to cybersecurity issues.

ICANN's role in the security of domain names and numbers has manifested itself through three main issues at policy and technical level: Domain Name System Security Extensions (DNSSEC[2]), Internet Protocol version (IPv) 6, and related to the privacy of data, the WHOIS information database. The issue of security for the Domain Name System (DNS) arose after security researcher, Dan Kaminsky, found a critical vulnerability in the DNS system in the summer of 2008. The DNS, basically, translates domain names that humans can remember for example, www.europa.eu, into the numbers used by computers (Internet Protocol (IP) addresses) to look up its destination within different levels of the directory service (each level managed by different entities for example, ICANN manages the first level or 'root zone'). What the Kaminsky incident exposed is the ability of any attacker to hijack the DNS process within any given level (in what is often termed as DNS cache poisoning or spoofing). Such spoofing allows attackers to 'take over control of a session to, for example, direct users to their own deceptive websites' (ICANN, DNSSEC, Fact Sheet 2011), where the user can enter confidential passwords and account details, or potentially be subject to attack through inadvertently downloading malicious software. There are also more serious variants of such attacks, whereby they are not localised but rather globalised redirections of Internet traffic. The classic case here is the case of the rogue Chinese name server that hijacked up to 10% of the Internet, routing it through China and subverting a proportion of the world's information flow to the automated web censorship regime in China (Klimburg 2011b, p.10).

The DNSSEC solution, which was operationalised in July 2010, is intended to counter the more serious threats rather than simply the spoofing, even though both have significant implications for security. At a basic level, it works through digitally 'signing' data (it does not encrypt data) so that users can be assured of its validity. In order for this technology to work effectively, however, it must be deployed at each level of the look up process from root zone (managed by ICANN) to

domain name (for example, dot eu managed by the EURID registry). In effect then, such a system rests upon the notion of 'trust anchors' to provide valid information at different levels (generic, national, sub-national and so on), and this is where problems may arise, which have implications for the *resilience* of the security governance provided by DNSSEC.

At a technical level, the threat of denial-of-service attacks would not be eradicated by DNSSEC, and might potentially make them more effective given that servers would be working with an increased workload (Klimburg 2011b, p.11). There is also the potential of contamination of the system through the spreading of false DNS information if ccTLD registries misidentify local trust anchors (Scott 2010). Furthermore, at a policy and governance level it is reliant on a commercial logic, which treats some of the symptoms, but is corrective rather than antidotal in nature. More specifically, although it allows the management of some risk in the form of spoofing and more severe hijacking of the DNS, even this is reliant on a cost-benefit calculation, in particular with regard to the management and administration of DNSSEC.[3] This is especially problematic for smaller ccTLD registries and registrars, but also those in less advanced countries where DNSSEC implementation is not even on the agenda (Mohan 2011; Klimburg 2011b, p.12). The problem is not just at the micro level, however. Indeed, the way in which DNSSEC is managed and governed at a macro-level by ICANN is not conducive to constituting a shared logic of action in the short term – in particular as it is reliant on voluntary compliance and 'crisis' to incentivise action among the stakeholders involved. Whilst there is no immediate solution to this, and many more registrars have signed up to DNSSEC since its introduction[4] moving to a mandatory – more hands-on meta-governance approach – could potentially incentivise many more stakeholders at different levels to implement DNSSEC. Indeed ICANN's generic TLD (gTLD) programme did this this at the registry level, with this purpose in mind and the hope that it would incentivise high-security authenticated zones to enforce the protocol at the second level too (Mohan 2011). Whilst there have been successful joint initiatives (for example ICANN and the Internet Society) to recruit more registries and other stakeholders to the DNSSEC initiative, not all are yet convinced of its efficacy or value in constructing a resilient DNS; additional incentives need to be provided if such actors are to think beyond the commercial logic to the longer term logic of sustainable security as resilience through the implementation of DNSSEC.

The issue of the transition from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6), and the issue of the WHOIS registry also have important security implications for ICANN in terms of how it governs such issues. The 'Internet Protocol' basically allows communication between different network devices on the Internet; you cannot be connected to the Internet without an IP number (32-bit number, written as '203.155.16.175'). When conceived IPv4 was thought to provide enough IP addresses (4.29 billion) for the foreseeable future. However the growth of Internet use across all dimensions of life – economic, political, social, military and so on – has led to the perception, that IPv4 will soon be depleted – with IPv6 (128-bit number) providing the scope for 340 trillion, trillion, trillion addresses. Such a transition then obviously brings with it both new security features (see http://www.ietf.org/rfc/rfc7123.txt), but also new opportunities for hackers and attackers given the potential foreseen and unforeseen problems and errors that are likely to arise during the transition (Klimburg 2011b, p.8; van der Steeg 2011). Whilst many commercial entities and leading countries such as China already have a clear roadmap for transition and operate secure dual IPv4/IPv6 capability, or IPv6 enabled equipment, others argue that it needs to be harnessed further, in particular in the military domain, if IPv6 is to provide a secure platform for effective future operations (see, for example, Yannakogeorgos 2015).

The problem for ICANN in terms of ensuring security during the switchover is that it is reliant on voluntary uptake of IPv6 by ISPs and TLD and ccTLD administrators, whilst at the same time, being responsible for the allocation of IPv6 addresses to the generic (for example, .org) and geographical TLDs (for example, .de,.uk) through the Internet Assigned Numbers Authority (IANA) function, with no way to actually mandate the switchover (Klimburg 2011b, p.8). In governance terms then, the voluntary nature of the switchover means that the transition period cannot be shortened as it is ultimately reliant on demand and resource, nor can the international uptake of IPv6 be enforced, making the Internet ecosystem vulnerable to attack. In terms of security as resilience, a model that is able to incentivise stakeholders to implement the changeover as quickly as possible is required, with some evidence that ICANN is fostering a closer relationship with governments in order to be able to secure the DNS through a more concerted action or hands-on meta-governance approach in the form of regulation if private actors do not comply.

The WHOIS information problem (the directory of website ownership) also raises similar issues of governance incapacity in relation to

what is a vital tool for addressing issues of cybercrime. It is problematic because although ICANN is responsible for defining user policy for gTLDs, ccTLD registries often define their own practices with regard to the sort of information that an owner needs to provide on purchasing a website, with registries also then responsible for providing WHOIS information. The issue is the difference in practices between countries, with those ccTLD registries that allow virtually anonymous registration most likely to be targeted for criminal purposes (for example, China). There is no simple governance answer to this, in particular given the debate, exacerbated by the Snowden revelations in 2013, on balancing the right to privacy with that of increasing intervention by states in the name of constructing a more secure cyberspace.

The WHOIS information issue is contentious, but in order to take it seriously and maximise flexibility it is clear that certain coherent codes or norms of conduct must be diffused across the key stakeholders – through facilitating and stimulating collaboration, or enforced regulation – the latter though unlikely to have resonance with those that offer an alternative model for Internet security and governance (discussed below). In summary then, it seems that various security issues have challenged ICANN's governance model at the policy level, and that ICANN itself, for some commentators (Weinburg 2010; Klimburg 2011b), has engaged actively with the discourse on public-private partnership and institutional isomorphism, in order to work more closely with governments and establish itself as an actor that is able and competent enough to provide effective resilient governance for the security of the Internet. Such a PPP model thus far has been suggestive more of hands-off rather than hands-on meta-governance, and thus it remains to be seen how far reluctant private actors will be incentivised into thinking differently about implementing new technology, in order to ensure effective security as resilience for the Internet.

Internet Governance Forum

The Internet Governance Forum (IGF)[5] was established in 2005 at the second phase of the WSIS process as a multilateral, multi-stakeholder, democratic and transparent institutional forum for discussing issues of Internet governance. The IGF mandate at the WSIS Summit in Tunis (2005) stipulated that it 'would have no oversight function and would not replace existing arrangements, mechanisms, institutions, or organisations, but would involve them and take advantage of their expertise. It would be constituted as a neutral, non-duplicative and non-binding process' (WSIS, Tunis Agenda for the Information Society 2005).

Importantly, the IGF was constituted as a body that would arrive at positions through deliberation rather than make decisions, where discussions were open, free and frank on any themes seen as important for the future of Internet governance, including issues relating to child protection, cybercrime and cybersecurity. Its normative strength has been in its inclusive and bottom-up nature, and in the fact that in its first five years, it has become a forum for learning through discussion of ideas that can be utilised in policy construction and development (Christou and Simpson 2012, p.104–105).

Given its institutional nature and the broad stakeholder make-up in the IGF, it is perhaps inevitable that the logics coming from the IGF on different aspects of cybersecurity will differ in emphasis and importance. However, having said this, it is clear from analysing workshop outcomes and IGF thematic reports between 2008 and 2014 (Security, Openness, Privacy) that particular security governance themes and debates are pervasive in the context of discussing potential approaches and models. Prominent among discussions have been: first, the relationship and balance to be struck between security, privacy and openness; second, what sort of governance model is suitable and effective for regulating issues related to cybersecurity in the context of the global Internet ecosystem. On the first issue, the debate has been not simply about balance but also proportionality. In this sense the discussion has been about degrees of balance not simply between security and privacy, but between individuals *as* individuals and individuals *as* part of a larger group. The broader political and legal context, of course, relates to ensuring the security of the state without eroding or transgressing individual rights and liberties, thus leading to a lack of trust in the Internet ecosystem in relation to identity, and specifically, the privacy of personal data.

This is a vexed and contentious governance issue as it is not just dependent on the different approach taken by states and cultures (for instance, the US and European approaches to privacy – see Chapter 7), but also between and within groups and networks that prioritise different principles according to their cause within different platforms. Security professionals in NATO and the technical community, for example, assert that a proportionate approach is possible at the physical and logic layer or level. Many human rights activists, privacy advocates and indeed Internet pioneers however, which view access to an open (stateless) Internet as a human right and principle, argue that anonymity should be prioritised over security, which they associate with intrusion and censorship. Within the IGF, given the varied representation from industry, public sector, civil rights groups and so on (Aspects of identity

yearbook 2011–12, p.24–29), the extreme views of either openness or security are only usually propounded by minority groups, whereas there does seem to be a broad majority that support the 'proportionality' principle. Having said this, it is not clear from the documentation available what this means in terms of a governance model at technical or policy level across all dimensions. What does seem to emerge though is a view that any framework that is constituted must be 'flexible enough to encompass the wide variety of approaches to rights and responsibilities of individuals, business and states that are found across the globe' (Ibid., p.28). The Edward Snowden revelations (of which more in Chapter 7), of course, have only served to sharpen up such a debate, and indeed call for a more accountable, transparent, democratic and rights-based approach to securing cyberspace.

On the second issue, the dialogue and discussion between stakeholders provides a tentative governance steer on how issues of cybersecurity and cybercrime should be regulated in order to provide flexibility and effectiveness. In this sense, the main threads of the many discussions (see www.intgovforum.org) point to a form of 'cooperative regulation' between all stakeholders, public and private, when dealing with issues of cybersecurity. As with the above debates on security, privacy and openness, however, there is a broad consensus on this, but also views on the margins on what such cooperation should entail. For some, at the policy level, it points to hands-off meta-governance where primary legislation is not needed, but rather coordination, facilitation and stimulation to indirectly influence partnership and cooperation through changing the environment. Hard regulation or hands-on meta-governance approaches are perceived to be too cumbersome and inflexible to keep up with technological developments and solutions, which often lead to unintended consequences. From this perspective, the multi-stakeholder approach represents the best way forward, in particular given the importance of engaging with and educating society and consumers in order to raise awareness of the risks and threats on the Internet. Others, whilst certainly in favour of multi-stakeholderism, also warn of the dangers of a multi-stakeholderism without a key role for governments. Neelie Kroes, former EU Commissioner for the Digital Agenda for example, expressed the view at IGF's opening ceremony in Nairobi in 2011 that,

> The fact remains that public authorities have a particular role. Indeed, a particular obligation to deal with public-policy matters off and online, and this must be reflected in the decision-making process.

> Otherwise, the outcome of multistakeholderism is that lobbyists hijack decision-making, that private vested interests trump the public interest, and that some put themselves above the law. These are not things I will accept now or in the future.
>
> (Kroes 2011)

This movement to a hands-on meta-governance approach to achieve resilience has certainly been a key feature of the EU's evolving cybersecurity approach. The EU initiative for a comprehensive Internet Security Strategy for Europe, for example, emphasised the need for 'one or more legal instruments therefore making an important step-up from the current voluntary towards a binding approach' (European Commission 2011), which was followed up by a mandatory approach within the proposed Network and Information Security Directive (2013) that accompanied the EU's Cybersecurity Strategy[6] (2013). The implications of this for moving towards security as resilience in Europe are discussed in some detail in Chapters 6 and 7.

Multilateral organisations and cybersecurity

Beyond the Internet governance institutions, multilateral fora have also been active in contributing to the evolution of resilient governance for cyber threats.

The G8 group of states

The G8 has addressed cybersecurity since the Okinawa Summit in July 2000 where it committed to strengthening cooperation in order to improve access to the Internet for the poorest and protect intellectual property rights. It has supported the draft Anti-Counterfeiting Trade Agreement (ACTA) and the work of the Organisation for Economic Co-operation and Development (OECD) on the economic impact of counterfeiting and piracy (French G8–G20 Presidency 2011). The G8 view on cybersecurity and Internet governance, reflected in the Okinawa Charter for the Information Society (2000), was of the private sector playing a lead role but with a responsibility on governments to create a regulatory and policy environment that is predictable, transparent and non-discriminatory. Discussions on cybersecurity regulation and governance really came to the fore though after 9/11, even though the Lyon Group (formerly Senior Experts Group on Transnational Organised Crime) was established in 1995, and expressed the need to review 'laws in order to ensure that abuses of modern technology that are deserving

of criminal sanctions are criminalised and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention and international cooperation in respect to such abuses are effectively addressed' (P8 Senior Experts Group 1996, p.4). It is claimed by Hart (2001) that in governance terms, the success of the Lyon group has stemmed from the participation of private interests, even though the main work was done by the law-enforcement agencies of the G8 governments. Indeed, and ironically, the initial 'heads primarily' format of the G8 gave it the flexibility to invite nongovernmental actors to discussions on security and other issues that required a multi-stakeholder approach.

One of the important subgroups created from the Lyon Group was the G8 Sub-Group on High-Tech Crime in 1997[7] (subsequently expanded to include non-G8 countries), which established the Ten Principles (see G8, http://www.cybercrimelaw.net/G8.html) in the combat against computer crime as a platform for ensuring that criminals are suitably dealt with in legal terms (as well as an Action Plan). The focus in governance terms has been on how to improve the legal environment within which to address cybercrime through further international sharing of information, cooperation and coordination between those authorities and private actors involved in enforcing criminal laws. Thus, this has not implied a sole role for public actors, but rather, the recognition that there must be cooperation between government and industry and that the industrial sector must be responsible for developing technical standards (governance) within global communications networks. Moreover there is a clear steer for the industrial sector, facilitated by the necessary legal frameworks, to develop and distribute secure systems and best practice in relation to personnel security, preserving electronic evidence, and ascertaining the location and identity of criminals (Communique, Justice and Interior Ministers of the Eight, 9–10 December 1997). On issues of mutual legal assistance and extradition, the emphasis has been on enhancing cooperation and coordination, and importantly, creating an international legal environment that is flexible enough to accommodate multi-jurisdictional cases, minimise constraints, and allow the necessary collection and sharing of evidence to prosecute cybercriminals.

The more recent discourse to emanate from the G8 on cybercrime and security supports more explicitly 'the multi-stakeholder model of Internet Governance . . . with flexibility and transparency . . . in order to adapt to the fast pace of technological and business developments and uses' (Deauville Declaration 2011). It also acknowledges the key role that governments must play in this multi-stakeholder model alongside regional

and international organisations, the private sector, and civil society in order to 'prevent, deter and punish the use of ICTs for terrorist and criminal purposes' (Ibid.).

Indeed there is an emphasis on all stakeholders, with governments, it seems, playing a key steering and facilitating role, to 'develop norms of behaviour and common approaches in cyberspace' (Ibid.) that embed within them the proportionate balance between security and privacy/individual rights. On intellectual property infringements and personal data specifically, the G8 positions again reflect the logic of the multi-stakeholder model, with governments creating the regulatory environment for action and implementation and the private sector at the forefront of driving initiatives. There is also, again, an emphasis on international cooperation and a 'common' approach based on consideration of national 'legal' frameworks and the right balance between individual rights and sharing personal data. Importantly and within the multi-stakeholder logic the G8 conclusions call for enhanced cooperation between all stakeholders (including users), and recognise the need for flexibility and transparency, to ensure adaptability to 'the fast pace of technological and business developments' (Ibid.). This bodes well for creating sustainable security as resilience, even though in practice, it seems, there is no clear agreement on which 'model' is more effective.

The United Nations (UN)

The United Nations is seen by many as the ideal interlocutor and platform for fostering the necessary dialogue and cooperative climate on cybersecurity. However, it also sits at the centre of a major debate on which international organisation should address issues related to cyber – including that of security. Essentially, and to oversimplify a little, there are those, such as Russia and China (and certain Arab countries) that operate with a 'sovereign logic' on matters of cyber threat that would like to see a global treaty agreed through the UN. Others, such as the EU, UK and US, argue that the UN (and the ITU as a UN agency) is not suited to Internet governance or leading on global cybersecurity governance given the slow and cumbersome nature of the decision-making process, and the rapid pace of technological development.

Beyond this debate, however, the UN, in particular the UN Office on Drugs and Crime (UNODC), the ITU and UNESCO have contributed to raising awareness on issues of cybersecurity and cybercrime, and provided recommendations which it has encouraged its members to adapt in order to improve their national cybersecurity resilience. Importantly, the UN Group of Governmental Experts on Developments in the Field of Information and Cyber Telecommunications in the Context of

International Security produced a report on cybersecurity in 2010 that provides recommendations on reducing cyber risk and protecting critical infrastructures nationally and internationally. Salient among those in governance terms was improved international cooperation between states, enhanced cooperation through measures to share 'best practices, manage incidents, build confidence, reduce risk and enhance transparency and stability', improved collaboration between state actors, private actors and civil society with cooperative actions and measurements to support this, and finally, capacity building in order to facilitate the improvement of security of other states in order to improve ICT security globally (UN Report 2010, p.7). The UN report on cybersecurity (2010) also provided important guidance on how cyber warfare issues are related to existing principles of international law (how international law applies to cyberspace). Further than this, in 2013 the UN Group of Experts on Cybersecurity 'for the first time at the UN level . . . was able to agree to an important set of recommendations on norms, rules, and principles of responsible behavior by states in cyberspace' (Volter 2013). Whilst this was no doubt an important step-change in terms of international consensus on a controversial issue which also included important recommendations on issues such as extending Confidence Building Measures (CBMs), building capacity globally and information sharing, it will rely on states embedding the central norms underpinning the agreement into practices, if a resilient and secure cyberspace is to truly emerge in the medium to long term. Evidence suggests that this is unlikely given the disagreements that still exist between states on key principles, which have only been exacerbated by the Snowden revelations in the debates and continuing work of the Group of Experts at UN level (Meyer 2013).

More broadly, the UN General Assembly produced five major Resolutions (see ITU 2011, p.17–18) on the issue of cybersecurity, with an emphasis on building trust in using ICTs in order to maintain and enhance the socio-economic benefits of ICTs for society. In resilient governance terms the resolutions steer towards a multi-stakeholder approach with strong legal frameworks to combat the threats of cybercrime and attacks on critical information infrastructures, and with a need for enhanced cooperation between states on these matters, as well as better coordination with all stakeholders.

International Telecommunications Union (ITU)

A fundamental role of the ITU, following the WSIS and the 2010 ITU Plenipotentiary Conference, was to build confidence and security in the use of ICTs. At WSIS, Heads of States and world leaders entrusted

the ITU to take the lead in coordinating international efforts in the field of cybersecurity, as the sole Facilitator of Action Line C5, 'Building confidence and security in the use of ICTs'. In response, ITU Secretary-General, Dr Hamadoun I. Touré, launched the Global Cybersecurity Agenda (GCA), which is a framework for multi-stakeholder international cooperation aimed at enhancing confidence and security in the information society.

The central tenets or pillars of the GCA are Legal Measures, Technical and Procedural Measures, Organisational Structures, Capacity Building and International Cooperation, with the aim to promote cybersecurity and maintain resilient and reliable information infrastructure (ITU Report 2011, p.20–21). In order to operationalise the GCA the ITU signed an agreement with the International Multilateral Partnership Against Cyber Threats (IMPACT), which supports, through its various Centres[8] the GCA achieve its strategic goals (see Ibid., p.21) including legal measures, organisational structures, developing strategies for the creation of a global framework for watch, warning and incident response, capacity building and international cooperation. Furthermore, ITU-IMPACT is underpinned by the 'partnership approach', with partners from Industry, Academia, International Organisations and Think Tanks. The ITU also signed a memorandum of understanding (MoU) with UNODC in May 2011 order to assist the ITU and UN members mitigate the risks posed by cybercrime. Activities have taken the form of joint assessment missions, conferences and training activities, with collaboration across the five pillars of the GCA. In line with the idea of public-private partnership, the ITU also signed an MoU with the Symantec Corporation, with the latter providing quarterly Internet Security Threat Reports in order to increase awareness of and readiness for cybersecurity risks among the ITU membership. Finally, under the GCA, the ITU launched the Child Online Protection initiative (November 2008), which has been established as an international collaborative network, providing guidance on safe online behaviour to relevant stakeholders.

In governance terms, the ITU has proposed a cybersecurity strategy model as a guide for member states to develop their own strategies (ITU 2008a, 2011), with an emphasis on multi-stakeholderism and coordinated local, national and global multi-sector action (see also ITU 2008). Within this context, the logics of this model are underpinned by the five pillars or platforms of activity already outlined above: Legal Measures, Technical and Procedural Measures, Organisational Structures, Capacity Building and International Cooperation. Indeed the justifications for

such a model are argued to be strategic, social and economic in nature, even though in practice, there might be a conflict between each of these logics as demonstrated in the case of the implementation of DNSSEC.

To elaborate further, it is clear that within the ITU model, there is an emphasis on governments as facilitators, even though it also argues that national governments should lead in setting any goals for cybersecurity strategy. In other words, whilst the ITU argues that all stakeholders have a role to play in elaborating and implementing strategy (from the judiciary to civil society, vendors and the intelligence community), the model does not suggest a key role for all stakeholders in the agenda setting stage. Indeed, the ITU recommends 'that Governments focus on setting the agenda and the conditions for all stakeholders to work together' with the agreed strategy then providing a platform for cooperation at all levels (ITU 2011, p.32). In terms of monitoring the effectiveness of the strategy, in governance terms, it is reflective of a classic regulatory state approach, that of appointing an independent agency. At a basic level it advocates a multi-pronged governance approach that includes hands-on legislation and hands-off incentives for collaboration within an overarching collaborative strategy constructed by national governments (for more details see ITU 2011).[9]

Interesting within the approach is the call for minimising bureaucracy in order to maximise flexibility and adaptability in passing legislation on cybercrime and cybersecurity (Ibid., p. 49–50), and establishing national security frameworks procedurally and technically as well as legally, in order to facilitate the development of common standards and solutions and a culture of cybersecurity. Importantly, it highlights the role of public-private partnerships in addressing the issue of cybersecurity given the involvement and role of different actors within the cyber sector. Indeed, on the latter, it is argued that successful collaboration between the public and private sector requires three elements: a) A Clear Value Proposition: that all stakeholders know exactly why collaboration is necessary and what the benefits are; b) Clearly Delineated Roles and Responsibilities: that these are agreed upon according to the overall strategy and its goals and the objectives of the stakeholders; c) Trust: that each party trust the others' motives and ability to fulfil duties (for example, on information exchange and privacy). The final elements relating to capacity building and international cooperation are cross-cutting pillars, but are nevertheless important to a sustainable and effective cybersecurity strategy, and the creation of a global culture of cybersecurity premised on a set of norms of behaviour for cyberspace. Significant here is not only capacity building in terms of the

professionals involved in cybersecurity activities, but also society, and indeed in terms of research and development in technologies to support robust and resilient cybersecurity strategies.

North Atlantic Treaty Organisation (NATO)

Whilst the first distributed denial-of-service attack against NATO's Public Affairs website occurred in 1999 (Tick 2010) and the protection of its information and communications systems was officially placed on its political agenda at the Prague Summit in 2002, it is not until the attacks on Estonia's public and private institutions in April and May 2007 that more urgency was injected into cyber defence. The war in Georgia in the summer of 2008, also further underlined the potency of cyber tools, demonstrating the potential for them to be used as a component of conventional warfare. The use of cyber tools in this way then, and the threat that they might also pose to the Euro-Atlantic community, further underlined the urgency and need for a NATO cyber defence policy for the alliance as a whole (www.nato.int/cps/en/natolive/topics_78170.htm) in terms of both the military and civilian aspects.

Since then NATO has done much to address the issue of cyber-attacks and highlighted the issue in its new Strategic Concept adopted at the Lisbon Summit in November 2010. NATO also adopted its new cyber defence policy in June 2011 (reaffirmed at the Chicago Summit in 2012). In parallel to the policy, a cyber defence Action Plan was agreed that will serve as the tool to ensure its timely and effective implementation. The policy offers a coordinated approach to cyber defence across the Alliance with a focus on preventing cyber threats and building the resilience of existing networks. Among other things the policy sets the principles on NATO's cyber defence cooperation with partner countries, international organisations, the private sector and academia (http://www.nato.int/cps/en/natolive/news_75195.htm). It also aims to bring all NATO structures under centralised protection with cyber defence being integrated into NATO's defence planning process, and outlines a framework through which it can assist, and collaborate with Allies with regard to intelligence, information sharing, and security interoperability based on a common set of NATO standards. The policy highlights the need for improving the security and resilience of Allies within NATO in order to strengthen in a sustainable way, the collective cyber defence policy – given that the latter can only be as strong as its weakest link. The policy further develops new political and operational mechanisms through which such a policy can be pursued, including the establishment of a NATO Computer Incident Response Capability (NCIRC) and

a Threat Awareness Cell for enhancing intelligence sharing and situational awareness. In addition, at NATO's Chicago Summit in May 2012, as part of a reaffirmation of the commitment to improve NATO's cyber defence policy, there was an agreement to bring NATO military and civilian networks under centralised protection – with the NATO Communications and Information Agency established on 1 July 2012 to facilitate this centralising process and enhance NATO's operational capability.

With regard to the institutional governance of its cyber defence policy, the North Atlantic Council provides the political oversight and takes decisions in cyber defence related crisis management. Below this, at the working level, the NATO Cyber Defence Management Board (CDMB) is responsible for the coordination of cyber defence throughout NATO's Civilian and Military bodies, and at expert level, the advice on the Alliance's Cyber Defence efforts and capabilities is offered by the Defence Policy and Planning Committee. MoUs exist between CDMB and national cyber defence authorities to facilitate sharing of information, dialogue and so on, and to inform NATO Rapid Reaction Teams on how they can support Allies in case of cyber crisis. The CDMB includes political, military, technical and operational staff that operate under the auspices of the Emerging Security Challenges division, with the NATO Consultation, Control and Command Board (NC3) the main body that is consulted on cyber defence in terms of the technical and implementation aspects. Finally, the NATO Military Authorities (NMA) and NATO Communications and Information Agency (NCI) are responsible for operational requirements, acquisition, implementation and operation of NATO's cyber capabilities, with the NCI Agency through its NCIRC Technical Centre providing technical and operational cybersecurity services throughout NATO[10] (www.nato.int/cps/en/natolive/topics_78170.htm). Beyond this, NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), established in Estonia in 2008, was set up to provide and develop training and education, and conduct research on legal and policy issues in the field of cyber defence. It is linked to NATO Allied Command Transformation and serves as a useful interface between NATO military bodies, academia, and the private sector. Moreover, it has a large outreach capacity, including NATO nations' cooperation with the EU. Indeed, the EU's ENISA and CoE CCD have organised joint events – sharing best practice that has emerged in the field – with this serving as a learning platform for preparedness in cyber defence issues. Moreover, the CoE CCD was also responsible for producing through the Tallinn Manual Process, the 'Tallinn Manual on the

International Law Applicable to Cyber Warfare' (2013), essentially setting out rules governing cyber warfare within the international legal context (Tallinn Manual 2013).

What then does this all mean in terms of the security logics that underpin NATO cyber defence policy? Whilst NATO faces the same general challenges on cybersecurity as many other organisations, its focus on cyber defence (and therefore primarily protection and deterrence) means that it also faces specific challenges in terms of its evolving policy, and the governance logics that underpin it. First, it faces the task of delineating more precisely what constitutes an attack, the use of force and an act of war in cyberspace. Second, there is the issue of putting into place a governance structure that allows timely and effective action against threats through a common set of standards and laws. Third, the creation of norms of behaviour to govern cyberspace, which requires the difficult task of harmonising national strategies through common understandings, and facilitating the sharing of information and threat mitigation, which member states are not always willing to do. Finally, there is the trade-off between protecting individual liberties and collective security which also exists more generally, but has particular connotations for NATO and its cyber defence policy (Noshiravani 2011, p.4).

Whilst NATO's approach to cyber defence is certainly comprehensive at first glance, suggesting a more coordinated, collaborative and inclusive policy than previously, with new supporting structures and learning through training and education at its centre to address individual and collective resilience, it also suffers from certain deficiencies. Put another way, there are certain obstacles that need to be addressed if it is to move forward successfully towards a security as resilience approach.

The first of these issues is that of the responsibilities of the different actors involved – in particular at member state level. NATO's emphasis is on collaboration with national governments to achieve harmonisation of standards and information sharing, but given the nature of the ownership of critical information infrastructure and cyber activity, this relies on effective public-private partnership at national levels. Although governments can no doubt develop a regulated standardised approach, it often has very different objectives to that of private industry that operates through an economic logic, and aims to deliver value to shareholders. In this sense, the private sector is often reluctant to move in the direction of the greater regulation of cyberspace – in particular given the difficulty for multinationals in navigating and indeed standardising the current complexity of regulatory legal measures that

exist across different cyber-related sectors. It is not impossible, of course, to incentivise the private sector to cooperate and coordinate in effective partnership (the Dutch model here, among others, is instructive), but this does require a common lexicon and a collective logic, as well as the issue of cybersecurity being elevated beyond the responsibility of ICT departments to the boardroom in many larger ICT companies (Ibid., p.5–6; IAAC Symposium September 2012). NATO's proposal for an Industry Cyber Partnership which members agreed on at the Cardiff Summit in 2014, aims to ensure that expertise and innovation from the private sector is exploited as much as possible in order to achieve the objectives of NATO's Enhanced Cyber Defence Policy and should go some way to addressing this issue if successful.

The second issue is that of obtaining clarity on the thresholds and standards that will apply to questions relating to: use of force in the cyber domain; when a cyber-attack can be labelled an armed attack (under Article 51 of the UN Charter and Article 5 of the Washington Treaty); what sort of action is permissible in response to a cyber-attack and which body of law applies to any such responses. Two issues are pertinent in this context. First, whilst there is much debate on this topic there is a general consensus that for a cyber-attack to be considered an armed attack it must have physical consequences – with the use of force being of a direct or indirect nature. Second, is the issue of attribution of blame in cyberspace, as the difficulty in identifying an attacker can affect the ability of states and organisations to respond in terms of timing and the relevant international legal framework, as well as the nature of any response to a cyber-attack (Ibid., p.6–7). Whilst the Tallinn Manual has gone some way to addressing the above issues; that is, it provides a mutual point of reference for definitions of military attack, the application of international law, distinctions between civilian and military targets, and methods of establishing which parties are or were involved in specific cyberspace conflicts it still falls short, for some, on resolving certain other salient issues. The manual, for example, does not provide clear criteria by which an attack can be defined as an act of war, arguing instead that this must be assessed case by case according to the gravity and potential effects of any decision. For Bendiek (2014, p.8) 'using international law to set up rules for cyber war just makes these kinds of actions seem more doable and . . . there is no precedent for norms that deal with conflict below the threshold of armed assault'. In addition, the exclusion of non-NATO experts from the discussion group that constructed the rules for cyber warfare has limited not only the scope but also the potential effect of such rules. Finally, for some, the

Tallinn Manual has scant regard for citizens' rights given that the broad definition of a military attack does not in principle ban governments from taking military action against non-state groups or even individual alleged hackers. From this perspective, the lines between police and military operations could become even more blurred, with ethical implications side-lined in the interests of cyber defence (Ibid., p.25)

A third issue is that of international cooperation and collaboration, especially with the EU given the overlapping membership of the two organisations. Indeed NATO–EU cooperation, if coordinated effectively, can certainly facilitate the emergence of security as resilience. Given the EU's ability to implement Regulations and Directives and NATO's ability to conclude international agreements, both agencies can contribute to the emergence of common standards, laws and practices that influence the direction and nature of international norms and principles for cybersecurity. Having said this, there are many impediments to effective NATO–EU cooperation in issues of cybersecurity which includes their different mandates and thus competencies, and the Cyprus–Turkey issue, placing legal limits on their ability to cooperate formally, at least (although not informally – see Chapter 6). In addition, given that both the EU and NATO have limited (geographical) memberships, any effective cooperation struck up between the two organisations would not address the needs or indeed reflect the preferences of the 'global' community of actors that operate in cyberspace and therefore seek to secure it. The implication here then, in terms of governance at least, is that any norms and principles agreed by the two organisations, in order to have global influence and relevance, would have to engage with other important stakeholders in the cybersecurity milieu, through other new or existing fora, and including the private sector and civil society.

Organisation for Economic Cooperation and Development (OECD)

The OECD in producing information on best practice with regard to critical infrastructure resilience is a useful tool for the EU and its member states in terms of developing their cybersecurity ecosystems. The OECD Working Party on Information Security and Privacy (WPISP) produces regular reports on resilience building, privacy, and the information society. Indeed, it has an established network of experts from government, business and civil society that serve to facilitate exchanges of information between stakeholders and to monitor activities in relation to cybersecurity (European Parliament Report 2011, p.19). In this sense, its governance structure is reflective of effective partnership and its steer in terms of best practice emphasises the need for a culture of

cybersecurity to emerge given the wider number of threats and risks now associated with information technology developments and increased interconnectivity.

To this end the OECD has produced a set of generic guidelines (2002)[11] intended to facilitate the movement towards a culture of cybersecurity. The approach advocated is inclusive, with the underlying rationale that 'each participant is an important actor for ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks' (OECD 2002, p.8). Moreover, it emphasises, consistent with the conditions set out in Chapter 2 for effective security as resilience, the need for guidelines to be adopted and implemented at policy and operational levels, and that 'efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy' (Ibid., p.9). In addition, it is argued in the report that factors such as leadership, in particular from governments (OECD 2003) and extensive participation by all participants is essential for creating an environment where security planning and management, and better understanding of the need for security is achieved (OECD 2002, p.8).

The OECD Report argues that the principles that underpin the Guidelines are not an attempt to provide a one-size fits all approach to the security of information systems and networks, but rather, 'to provide a framework of principles to promote better understanding of how participants may both benefit from, and contribute to, the development of a culture of security' (Ibid., p.14). In other words, the principles represent a set of conditions that if implemented in policies, practices, measures and procedures, are most likely to create the type of environment whereby security as resilience, including prevention and reaction, will become embedded at all levels and amongst all active participants in cyberspace, individually and collectively. Of course it can be argued that such principles whilst broadly acceptable for most Western audiences (for example, the principle on democracy) are fiercely contested among those countries, organisations and individuals that operate under different government and security logics, as demonstrated with the Council of Europe Cyber Crime Convention (discussed below). It can also be argued that some of the guidelines do not go far enough; for example, the principle on response states in connection with cybersecurity incidents that, 'Where permissible, this may involve

cross-border information sharing and co-operation'. Such sharing of information across borders is a pre-requisite for security as resilience – and a norm that all participants involved in cybersecurity should adopt and operationalise in order to ensure effective reaction and response to cyber incidents. Finally then, such guidelines are voluntary in nature, and whilst providing a generic framework for the creation of a culture of cybersecurity, do not provide principles that are universally acceptable, or indeed that have been universally adopted and implemented by all participants. Indeed, the world in 2015 is even more complex than in 2002, with the OECD also active in providing more specific recommendations for policy measures by Internet service providers against botnets, underpinned in governance terms by private sector initiatives and public-private partnerships (OECD 2012).

Council of Europe

The Council of Europe's (CoE) central contribution to the governance of cybersecurity comes in the form of the Convention on Cybercrime which was agreed in 2001 and entered into force in July 2004. Also commonly referred to as the Budapest Convention, it is politically important and is the only binding agreement on cybersecurity issues, which has been drawn on for best practice within and outside Europe. At the time of writing (March 2015) 45 countries (including the US) have signed and ratified the convention, which includes 24 EU member states[12]; a further eight countries have signed it without ratification.[13] Having said this, it is also subject to contestation given its call for international cooperation and information sharing – including cross-national and trans-boundary cooperation between police forces. Countries such as Russia and China (as well as certain developing countries) have stated their clear opposition to ratifying the convention due to the concern that it would undermine national sovereignty, which is certainly problematic to achieving global security resilience given the number of Internet users in these countries and the fact that they are the alleged source of many cybersecurity breaches and attacks in recent years.

In governance terms, the Budapest Convention is voluntary in the sense that it is not mandatory for all states, in particular outside Europe, to sign up to it. Its purpose, however, is to establish 'a common criminal policy aimed at the protection of society against cybercrime' (Convention on Cybercrime 2001, Preamble). In order to achieve this it requires those that have signed up to the convention to adopt and implement legislation on the procedural aspects of cybercrime, such as illegal access and interception, misuse of devices, fraud, forgery, intellectual property

(IP) offences, interference with data and systems and child pornography. Moreover, it provides a transnational legal and law enforcement framework that requires signatories to adopt laws concerning the investigation of cybercrime, and to cooperate, via extradition and mutual-law enforcement assistance, in the investigation of such crimes with other countries. In addition to the Budapest Convention the CoE Parliamentary Assembly has also provided recommendations on the Internet and Law, and expounded the view that whilst the nature of the Internet makes it impossible to regulate, an Internet code of ethics should be established through use of a legal instrument and the establishment of a European Internet ethics authority, in order to induce 'civic' behaviour on the Internet through the establishment of basic rights and duties of Internet users (CoE Parliamentary Assembly Recommendation 1670, 2004; O'Neill 2012, p.8).

Whilst the EU has clearly bought into and deferred to the CoE's Budapest Convention with regard to cybercrime, which is also reflected in the Stockholm Programme for internal security (2010, p.22), there is much debate on its efficacy, related in particular to its lack of enforcement mechanism when signatories fail to meet their obligations under the terms of the treaty. Moreover, weaknesses remain in the context of the EU's 28 member states, not least because whilst the CoE 'Convention remains the only international legal instrument to date', it nevertheless, 'shows weaknesses due to the fast-moving developments in cybercrime' (European Commission 2010, p.157 final). Such weaknesses include the lack of reference on how to deal with large-scale cyber-attacks as well as structural and cultural problems related to the functioning of national contact points in the context of cooperation in cybercrime.

More broadly, a central issue relates to the international nature of cybercrime, and the problem already alluded to above with regard to contestation. Cybercrime is a global problem requiring global cooperation if a robust security as resilience is going to emerge, and therefore the CoE Convention as a tool for combating cybercrime can only become truly effective if countries outside Europe sign up to the norms that underpin it.[14] The Global Project on Cyber Crime has been established for just this purpose – to promote the Convention beyond Europe – and has had partial success in terms of certain countries in Asia and Latin America drawing on the convention and implementing legislative reforms based on it.[15] Others still posit and propose an alternative view, grounded on alternative norms and principles. The Shanghai Cooperation Organisation nations (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan) for instance, have an agreement in

place – the International Information Security Agreement – that emphasises a primary role for national security and the primary role of the state in controlling information technology and managing risks and threats. Moreover, it sees Western nations and their dominance of the information space as a major threat to them, their socio-political systems and cultural way of life (Goldsmith 2011, p.4). Similar to other norms and tools invented in Europe and the EU, the convention embodies many useful principles for ensuring effective security as resilience, but agreement and implementation beyond Europe is critical if it is going to have any real impact on cybercrime given its global nature.

Organisation for Security and Cooperation in Europe (OSCE)

Discussion of a comprehensive approach to cybersecurity in the OSCE forum was driven by the Estonian Chairmanship in 2008 following attacks on its own systems in 2007. Prior to this the OSCE focused on enhancing different aspects of cybersecurity, for example. cybercrime, cyber terrorism, and on efforts to ensure 'freedom' of assembly, expression and information on the Internet. Since then, activities have included high-level meetings and conferences on strategic cybersecurity issues and a comprehensive approach, but with no exact agreement on what role the OSCE can play.[16] One fruitful discussion to emerge in this context is that for the development of norms on state behaviour for cyberspace, a notion which has also been discussed in other multilateral organisations (as shown above). An OSCE conference in May 2011 also explored questions of how the OSCE mandate might be strengthened to enhance its international role in cybersecurity, as well as possibilities for developing internal OSCE mechanisms in cybersecurity and an elaboration of an OSCE strategic document on a comprehensive approach to cybersecurity.[17]

However, membership of the OSCE, which brings together countries from North America to Central Asia, including member states of the EU, NATO and Commonwealth of Independent States, means that there are a diverse range of normative visions and strategic approaches to security resilience in cyberspace. Thus, whilst at the OSCE level there has been progress on agreeing an initial set of CBMs for cyberspace which suggests its broad membership is an advantage and not an obstacle to achieving consensus on certain issues, that very same advantage dissipates precisely because of its diversity, and, of course, because China is not a member of the OSCE (European Parliament 2011, p.20).

A good example of this is the contrast between UK (see Downing 2011; Hague 2011) and US (and other Western states and International

Organisations [IOs]) proposed norms for cyberspace on the one hand and those of Russia and China on the other. As expected, there is convergence and overlap between the UK, US and ITU positions, in particular if we focus on the dimensions of universal access, approaches to cybercrime, international collaboration and the principle of upholding fundamental freedoms. If we compare the principles advocated by the US, UK and ITU to those of the Shanghai Cooperation Organisation (SCO), then we can observe different logics at play with regard to the norms advocated for state behaviour in cyberspace (Healey 2011a), whilst also noting some element of convergence. Although the SCO agreement (2008) did not explicitly discuss norms, it emphasised 'state control'; indeed in previous proposals from Russia there was a clear and predictable steer to the limitation of cross-border flows of information because of the impact that this might have on the culture of security. Developments since then have seen a very broad consensus emerge between Russia, China, the US and the UK on some of the general principles and norms for governing cybersecurity such as confidence-building (as noted above), but such discussions have avoided the more controversial issues of content and information control (UN Group of Government Experts Report 2010).

In September 2011, members of the SCO (Russia, China, Tajikistan and Uzbekistan) proposed that the UN Secretary General facilitate a dialogue around their new draft proposal, the 'International Code of Conduct for International Security'. This was drafted as a formal document of the 66th session of the UN General Assembly, with the express purpose of it being used to reach a consensus on international norms of behaviour for the Internet. This Code of Conduct (see http://news.dot-nxt.com/2011/09/13/china-russia-security-code-of-conduct) raises a series of basic principles, which at first glance do not seem divergent from what is being advocated by the US, the UK and the ITU (Healey 2011b). For example, complying with the UN charter, international infrastructure and a commitment to ensure supply chain security are all 'norms' that chime with many of the principles proposed by the US and UK. Despite this, however, a deeper look at the security logics behind the proposal also raises potential points of concern for many that advocate a multi-stakeholder approach to cybersecurity and the preservation of freedom of access, expression, and information. Sceptics have argued, for instance, that the emphasis on promoting the 'establishment of a multilateral, transparent and democratic international management of the Internet', and the expected commitment to '. . . prevent other states from using their resources, critical infrastructures, core technologies

and other advantages, to undermine the right of the countries . . . to independent control of ICTs, or to threaten other countries' political, economic and social security', and 'To cooperate in combating criminal and terrorist activities which use ICTs including networks, and curbing dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment', are underpinned by a sovereign logic of control rather than freedom and resilience.

In terms of the first of these codes, promotion of the ITU to take a lead role in Internet governance, that is, a move to a traditional intergovernmental model, could lead to the Balkanisation of a spate of national Internet spaces, rather than multi-stakeholder governance; and China would also acquire greater weight and influence in terms of voting behaviour through the UN system. This also has implications then for the notion of security as resilience for all and an emergent culture of cybersecurity if other actors are side-lined in favour of a state-led, constructed and enforced approach. For the second and third of these codes, given the previous commitments by members of the SCO to limit information flows if it impacts on their own security, alongside the perceived dominance of the US in controlling the Internet, there are concerns that it would provide justification for repressive regimes to further limit free speech and access to independent external news sources, as happened during the Arab uprisings in Egypt and Libya (see also Gjelten 2010). Moreover, it might also provide an excuse to introduce draconian laws on access and dissemination of information that might threaten national security (Healey 2011b). Finally, there are also further concerns about what is not visible in the Codes of Conduct, including, for example, no commitment to control patriotic hackers supported by states that are seen to be at the centre of cyber conflict, and of which Russia and China are seen as sponsors.

Conclusion: Security as resilience in the international cyber ecosystem

Many guidelines and debates exist at international level on how governments and organisations can create security as resilience through a variety of governance methods, forms and modes. It is also evident, however, that among the stakeholders involved, there is still much debate as to how security as resilience should be achieved, in particular in relation to the fundamental rights and security balance debate.

The Snowden revelations have only served to exacerbate argument on such a balance, and provide justification to states that have used a national security first approach to enforce a security of control around their Internet space. Aside from this, there is also somewhat of a tension between the commercial logic and the security as resilience logic (Type 3) that at the moment is not adequately addressed in terms of the meta-governance of regulation, as well as between the sovereign logic of certain states and the open multi-stakeholder approach advocated by many leading states and international organisations.

There is a clear recognition in the international community that global norms to govern the behaviour of states and other actors are required if a global culture of security is going to emerge in cyberspace, and there are also very clear guidelines and a broad consensus on some of the key principles that should underpin any global framework. Indeed progress has been made by the UN Group of Experts on the applicability of international law; the Tallinn Manual was published, and CBMs were agreed at the OSCE. However, whilst there is certain convergence at the level of broad principles, consensus is far from apparent when analysing the logics of resilient security governance that underpin the construction of the more specific aspects of such principles, and the policy prescription that results from them across different state borders. Indeed, it is apparent that how cybersecurity is perceived between and within levels by the different international actors creates both opportunities and constraints for achieving security as resilience in a truly global sense – which is critical given the borderless nature of the cybersecurity problem.

Moreover, this points to the importance of the politics of security resilience being at the centre of the debate in the development of an effective global ecosystem. The tensions and contradictions at the centre of the different logics within the (geo)politics of cyberspace – represented within various codes of conduct, guidelines, principles and international laws and charters constructed and agreed, are what the EU must continue to engage with, draw from and effectively connect with and shape, if its own efforts to create a comprehensive ecosystem of resilient security governance are to bear fruit. It is already evident that the EU, in constructing its current positions, is embedded within the broader global ecosystem: the chapters that follow will provide an analysis of how such existing global norms have been shaped by and helped to shape national and EU strategies within the different facets of cybersecurity.

4

National Cybersecurity Approaches in the European Union: The Case of the UK

Introduction

The European Union (EU) has accelerated the development of its cybersecurity strategy since February 2013, which has inevitably also brought under greater scrutiny the variation in cybersecurity resilience and preparedness across the EU member states. Just as with the EU context that will be analysed in the chapters that follow, national levels of preparedness across Europe are perhaps the most important dimension of the cybersecurity ecosystem that if not improved to at least meet minimum standards could impact negatively on the ambition of achieving an effective EU cybersecurity strategy. Indeed the EUCSS was constructed *to facilitate* the security of cyber resilience in EU member states, in the recognition that it was national governments that could primarily drive the process of improvement and transformation in the cybersecurity ecosystem within Europe.

Whilst an overview of 28 EU member states would provide us with a clear idea of the emerging conditions for cybersecurity of resilience across the EU, comprehensive research on this issue, across the different levels and layers of cybersecurity preparedness is sparse, with the last major study undertaken at the time of writing by ENISA in 2008 (ENISA 2008), and updated in 2010 (ENISA 2010). Such studies of country preparedness related to cybercrime, cyber-attacks and network resilience have revealed a great deal of variety and divergence across the European space – that is, EU member states and the European Economic Area (EEA) countries (Iceland, Lichtenstein and Norway) – in terms of information exchange and cooperation modes and mechanisms as well as security incident management and reporting, risk management and

emerging risks, network resilience, privacy and trust and awareness raising (ENISA, Key security actors, strategies, & good practices in Europe mapped 2010).

Indicative of the divergence that exists in Europe, although also how far many countries have come in a short space of time, is that 18 EU member states have a cybersecurity strategy,[1] compared to a handful of countries just five years hence. Indeed the general trend indicated in the ENISA country reports,[2] is that of progressive learning within the variety that exists – facilitated in particular by diffusion of good practices that exist in leading member states. This is not to say that member states are in any way nearing convergence in practice, but rather that a common understanding of at least the minimum standards required for effective security as resilience is beginning to emerge.

In this sense, and beyond these reports, it is clear that there are certain leaders when it comes to cybersecurity good practice (for example, UK, the Netherlands) and there are those that are evolving at a slower pace due to a number of reasons – resource, size, knowledge, culture and so on (for example, Malta, Portugal, Slovenia) (Interviews, ENISA 2012; EEAS 2013; European Commission 2013/2014). Whether leaders or late developers in terms of cybersecurity capability and preparedness, each member state has different historical, social, economic and security concerns and therefore perceptions and needs when it comes to cybersecurity resilience. This makes the task of achieving an effective security as resilience complex, and one that can ultimately only be achieved in the long term if the necessary conditions are constructed across Europe and beyond, given the global nature of the issue (see Chapter 3).

As the task of a comprehensive review of the EU member states is not possible in a single chapter (perhaps not even in a single volume!), the focus here will be on an in-depth analysis of a leading member state[3] case study that can potentially offer examples of good practice for the rest of Europe. Whilst reference to other member states will be included wherever appropriate throughout the chapter to add a comparative element, the main analysis and assessment will be on UK efforts to achieve cyber resilience – the strengths and weaknesses of the UK approach, and what lessons can be learnt from its policies and actions within Europe. This chapter will seek, overall, to provide a clear idea of where the UK is in its development of effective security as resilience, and how this relates to the evolution and implementation of EU cybersecurity policy and strategy. The first section will provide a context within which to understand the evolution of the UK approach to cybersecurity. The second

section will then focus on and assess the UK cybersecurity strategy, and in particular how far actions taken to achieve its main objectives can offer lessons through good (and perhaps not so good) practice. The chapter will conclude on the implications of the UK approach for its own cybersecurity resilience, and for good practice potentially being transferred or diffused across Europe.

The UK's evolving narrative on cybersecurity

Cybersecurity in the UK has been driven by several logics over the last five years: first, by the perceived threat to national security and the potential of this threat to disrupt networked, digital activities in military and security terms; and second, the broader economic, political and social implications of cybersecurity threats given the increased reliance of many individuals, businesses, and critical infrastructure providers on cyber-based (ICT) systems. Such logics have been underpinned by a narrative that has evolved within the UK's Strategies for Information Assurance, National Security Strategies (NSS) and Strategic Defence and Security Reviews (SDSR), culminating in its updated Cyber Security Strategy (CSSUK 2011[4]) which spelt out in some detail the main dimensions of the UK government's National Cyber Security Programme (NCSP).

For example, there was recognition early on of the threat by non-military means, focused in particular on state-led threats to the UK via cyber-attack or cyber espionage (NSS 2008, p.16). This initial narrative was focused on cyber defence and developing cyber offence in relation to state-sponsored cyber-attacks; and very much influenced by the 2007 cyber-attack on Estonia's public and private systems and infrastructure as well as the cyber-attacks on Georgian infrastructure in 2008 during the (conventional) Russian military offensive in the country. However, it was also clear that the cyber threat was understood in broader terms and that the effective functioning of cyberspace was essential not only in terms of the defence dimension, but also with regard to citizens, business and government being able to exploit the opportunities that cyberspace presents in the economic, social, cultural and political sphere (Cyber Security Strategy of the UK 2009; Digital Britain 2009).

To this end there was recognition that certain measures and new institutional structures had to be established and developed in order to ensure a more effective security as resilience in the UK. For example, the CSSUK (2009, p.3) spoke of the need for 'a coherent approach to cyber security, and one in which the Government, organisations across all sectors, the public, and international partners all have a part

to play'. Of course there were a number of other existing organisations that were tasked with dealing with cyber threats, most important including: Communications-Electronics Security Group (CESG which was part of Government Communication Headquarters (GCHQ)) which ran the Computer Emergency Response Team (GovCertUK) that acted on behalf of the public sector to provide warnings and assistance in resolving serious IT incidents and also provided the National Technical Authority for Information Assurance; The Centre for the Protection of National Infrastructure (CPNI) which played a similar role to GovCertUK but for business and UK critical infrastructure providers; and in terms of cybercrime the Home Office, Serious Organised Crime Agency (SOCA) and police (important here was the Police Central e-crime Unit established in 2008) worked together through initiatives such as the Association of Chief Police Officers (ACPO) e-crime strategy (see below). However, it was felt that in order to achieve more effective resilience, a central cybersecurity capability was required and this was subsequently created for the first time in the UK[5] through the establishment of: The Office of Cyber Security (set up in the Cabinet Office) for the purpose of providing greater coherence and leadership strategically across government; the Cyber Security Operations Centre in GCHQ to monitor and coordinate incident response, enable a better understanding of attacks against UK networks and users and provide better advice and information about the risks to business and the public (Ibid., p.5).

Beyond this, the underlying principles outlined in the CSSUK (2009, p.9–11) certainly pointed to an understanding of the conditions required to create a more resilient UK cyber ecosystem. For instance, there was an emphasis on engaging with all stakeholders through partnership and retaining strong, balanced and flexible capabilities, as well as working with international partners in order to ensure a global, rule-based environment for addressing issues of cybersecurity. The new cyber structures and principles were seen as key for achieving the workstreams that were identified to drive change forward in order to achieve a better security as resilience. This included not just enhancing preparedness and protection, and improving the legal, regulatory and policy environment domestically and internationally, but also, and importantly, awareness and cultural change. Indeed, instilling the necessary changes in cyber culture and 'embedding cyber security in wider aspects of policy formulation' were important objectives within this workstream. In addition to this there was a recognition that skills and education needed to be enhanced to meet skills gaps, that an industrial strategy for cybersecurity had to be developed, that cybersecurity was a global issue that needed

coherence beyond the UK, and that an understanding of what was required in terms of capabilities and governance to ensure effective security as resilience, would have to be improved (Ibid., p.18–20).

The Labour government in the UK then, constructed an initial platform and the principles for building an effective security as resilience, and had a practical awareness of the conditions they had to foster to achieve a mature level of resilience in the UK. Having said this, it was also the case in practice, despite certain achievements (with regard to e-crime for instance), that there were serious shortcomings for achieving such conditions within the existing structures – not least in terms of the skills, expertise, leadership and resource to establish a resilient ecosystem and indeed the culture of understanding, cooperation and coordination that was required within government, between government and other stakeholders and between the government and international partners.

Thus a key challenge for the UK coalition government (Conservative/Liberal Democrat) that came to power in May 2010 was to build on this approach, raise the profile of cybersecurity further (Downing 2011, p.9) and provide the resource and narrative that would convince all stakeholders that cybersecurity had to become a national security priority. Indeed it seems that despite the ambition and understanding from certain elements in government to create a more integrated approach to constructing cybersecurity resilience there was much still to do on a cultural level to persuade certain government departments beyond the Ministry of Defence (MoD) and GCHQ, as well as the private sector that the cyber threat had to be understood in broader (economic and social) terms, thus requiring the involvement of a range of stakeholders (Neville-Jones[6] and Phillips 2012, p.32). In addition to this lack of skills and expertise, lack of resource was highlighted as a key barrier to developing more effective responses, in particular with regard to cybercrime (Downing 2011, p.10). There was also a certain perception of the central response mechanism as fractured and incoherent, with information-sharing between public and private sector actors in need of improvement in terms of quality and quantity. The approach in the UK, certain evidence suggests, was not as comprehensive as it needed to be; with a cultural shift needed in the public and private sector in order to ensure a more effective security as resilience (Cornish et al. 2011, p.viii).[7]

Accelerated prioritisation of cybersecurity was achieved through what certain scholars might describe as securitisation of cyber (in)security (for example, see Dunn Cavelty 2008a, for the US case) – with carefully selected examples demonstrating the increasing degree to which e-crime

had affected key government departments such as the Department for Work and Pensions (DWP), and more broadly, the theft of intellectual property such as information regarding the design and performance of the F-35 Joint Strike Fighter (Neville-Jones and Phillips 2012, p.32). Such examples were used during the SDSR to convince government departments of the urgency in which cybersecurity needed to be treated, culminating in cybersecurity being elevated to a tier one risk in the UK National Security Strategy (UKNSS) of October 2010, thus making it a national security priority. To this end it categorised 'hostile attacks upon UK cyberspace by other states and large scale cybercrime' as one of the priority risks alongside military crises, major accidents and natural hazards and terrorism (UKNSS, p.27). These priorities also reflected the EU's Strategic Priorities for its Internal Security (The EU Internal Security Strategy 2010). Finally, new money was allocated to (only) cybersecurity in the SDSR – a sum of £650 million over a five year period. Indeed, as part of a spending review in 2013, an additional £210 million was allocated for new and existing cybersecurity projects – increasing the total budget for the programme to £860 million (to be spent by March 2016).

The UK cybersecurity strategy: Building effective security as resilience?

What then were the central objectives of the strategy that was constructed by the coalition government in order to enhance cybersecurity resilience in the UK? Moreover, how has the UK cybersecurity programme evolved in practice to create the necessary conditions and governance mechanisms for cybersecurity resilience? What lessons can be learnt from the UK experience and evolving practice for the rest of Europe?

As already alluded to above, the UK Cyber Security Strategy (UKCSS 2011) was revised in 2011 with a single vision and priorities broken down into four core objectives. The vision reflected dominant driving logics and was 'to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society'. There was also a clear public and private sector element to the strategy with priorities broken down into the following (UKCSS 2011, p.8):

1. The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace

2. The UK to be more resilient to cyber-attacks and better able to protect our interests in cyberspace
3. The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies
4. The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cybersecurity objectives

In general, the UKCSS (2011) signified a step-change institutionally and in terms of resource for addressing cybersecurity issues. In addition there was recognition that central leadership and coordination was important – with responsibility for cybersecurity moving from the Security Minister in the Home Office to the Minister for the Cabinet Office and Cyber Security.[8] Furthermore the issue of partnership and effective collaboration was recognised and prioritised across several dimensions: from leveraging the support of the private sector and academia to co-designing credible policy; to creating platforms for more effective sharing of real-time data to enable swifter responses to cyber-attacks; ensuring that appropriate standards (risk-management regimes) are implemented across the private and public sector; building effective international connections given the global, borderless nature of cybersecurity; and finally, ensuring that the necessary up-skilling and educational programmes are constructed in order to ensure that expertise is developed across the many facets of cybersecurity to be able to meet cybersecurity challenges in the short, medium and long term (for example, forensics, surveillance, information assurance and so on).

There is also an individual element to this educational dimension in terms of raising awareness and enabling citizens to be safer online and to more easily identify and use mechanisms for reporting cybercrime. From a governance perspective it is clear that overall the UK government places emphasis on hands-off meta-governance – that is, incentivising the private sector rather than mandatory regulation – which is in line with its approach to the regulation of the Internet more broadly (Telephone Interview, UK cybersecurity official, October 2014). Indeed, as one official put it, the UK is 'trying to stimulate a self-sustaining market around cyber security' intervening directly only where there is justification to do so in the case of market failure (Telephone Interview, Cabinet Office official, October 2014). This sits in stark contrast to the underlying idea of the EU's proposed Network and Information Security Directive, which suggests mandatory reporting for all sectors which are deemed to be owners of critical infrastructure (see Chapter 6 for details).

Cybercrime and making cyberspace safe for UK business: Institutional innovation and improved partnership?

Historically in the UK the first institutional response to cybercrime was the National High-Tech Crime Unit (NHTCU) in 2001, alongside which were established 43 local HTCUs at police force level. However, this central response to address cybercrime directly was short-lived when the NHTCU was absorbed into SOCA in 2006. Effectively, this left a gap and reduced focus at national level within the police service with regard to e-crime prevention issues and – critically – eliminated a central coordinative mechanism with regards to resources for e-crime. In addition, capability to investigate large-scale cybercrime was reduced in areas that did not fall within the remit of SOCA (ACPO e-crime strategy 2009, p.1).

The importance and prominence of cybercrime led to the creation of the ACPO e-crime portfolio and Home Office funding of £3.5 million for the establishment of the Police Central e-crime Unit (PCeU) in 2008 under the leadership of the Metropolitan Police Service (MPS).[9] In addition the National e-crime Programme (2009) was created to coordinate the increasing number of e-crime initiatives emanating from the ACPO e-crime portfolio, and the ACPO e-crime strategy was developed to communicate the MPS strategic approach to e-crime. Whilst it was acknowledged that the PCeU was relatively successful in addressing e-crime (Interview, former PCeU official, August 2014), and in setting up models of good practice with regards to information sharing with business (through the *Global Virtual Task Force*, for instance: see Cornish et al. 2011, p.19), it was equally obvious that there was an issue in terms of limited resource and the lack of standardised training across the police and expertise to deal with cybercriminals (Interview, former PCeU official, August 2014; Downing 2011, p.10), as well as a 'lack of cohesion' between the organisations established to tackle cybersecurity (Hopkinson[10] cited in Shah 2012).

The UK Cyber Security Strategy (2011) and the NCSP introduced with it, sought to overhaul the approach to cybercrime in order to address the central shortcomings identified, and to provide further centralisation, coordination and strategic as well as operational effectiveness in tackling cybercrime. Thus, the National Crime Agency (NCA) was established with four pillars of action: Organised crime, Border policing, Economic Crime and the Child Exploitation and Online Protection Centre, with the newly established (operational in October 2013) National Cybercrime Unit (NCCU) housed within the NCA and overlaying the central pillars. Essentially the NCCU replaced the PCeU, and in doing so also recognised cybercrime as a crime in itself and a tool

for the execution of other crimes (The National Crime Agency 2011). In addition, nine Regional Organised Crime Units (ROCU) were established across the country with cyber teams based in each of them in order to facilitate the fight against cybercrime; and more specifically, run investigations, and provide advice and support to business and the public across their regions.

Whilst this new structure has, according to the head of the NCCU led to more effective strategic leadership with regard to harnessing skills and partnerships across government, law enforcement and industry in the UK and internationally, leading to a string of successful operations (The National Security Strategy, Our Forward Plans 2013, p.5), there are clearly still many challenges with regard to creating effective conditions for security as resilience with regard to cybercrime. For example, the National Audit Office Report (Update on the National Cyber Security Programme 2014, p.11) points to the lack of qualified personnel and technical capability within the NCCU and the cyber teams within the ROCUs to deal with the observed levels of (increasing) cybercrime. Whilst it could be argued that such issues are being dealt with through further investment to provide specialised training and increase capacity with regard to frontline support, and coordinated centrally by the ACPO national policing lead (The National Security Strategy, Our Forward Plans 2013, p.5), others still point to problems with regards to the lack of any standardisation of such training and a lack of mainstreamed cyber training embedded and integral to general police officer training. Indeed a central lead on this does not resolve the issue of where each regional lead 'buys' training from – and thus ensure that the right skillsets are actually being acquired across the relevant dimensions of cybercrime: prevention, detection, investigation and prosecution. Moreover, if a culture of cybersecurity is to be embedded and mainstreamed at all operational levels, then this must be remedied and a more comprehensive approach to training implemented (see, for example, Tightening the Net 2015).

Beyond this the UK government have sought to engage more effectively with the relevant stakeholders domestically and internationally in order to eliminate the cybercrime threat. Domestically the Home Office Cyber Crime Reduction Partnership (CCRP) was established which has sought to bring together government, industry, academia and law enforcement agencies – led by the Home Office and the Department of Business, Innovation and Skills (BIS) – to coordinate efforts on cybercrime and more specifically, seek opportunities to work in partnership in order to provide practical help to small and medium-sized

enterprise (SMEs) and citizens and potentially design out cybercrime. Internationally, the UK has also led on creating innovative collaborative arrangements – of an ad hoc and more institutionalised nature – to tackle different types of cybercrime (issue driven action).

For example, in the fight against bank theft malware, and more specifically to combat the Shylock Trojan,[11] the NCA brought together partners which included the FBI, Europol, BAE Systems Applied Intelligence, GCHQ, Dell Secure Networks, Kaspersky Lab and the German Federal Police. The operational aspects were conducted from the operational centre at the European Cybercrime Centre (EC3), and importantly from a security as resilience perspective, allowed effective collaboration between cyber investigators, coordinated by the NCA and supported by the necessary organisational country partners involved (UK leads international partnership to fight cybercrime, 2013).

In an extended more institutionalised pilot of this arrangement the Joint Cybercrime Action Task Force (J-CAT) was established in September 2014 at EC3 led by Andy Archibald, the deputy director of the UK NCCU. J-CAT, despite its relative newness, experienced operational success, but has also highlighted important issues – for the UK and other EU member states (as well as non-members) that need to be dealt with if the conditions for effective partnership and collaboration are to be embedded across the European space. One such issue relates to the legal layer and how evidence can be accessed in real time. In certain EU countries (which tend to be police-led such as the UK) access to internet protocol addresses, for instance, can be gained fairly quickly,[12] whereas in others, where police officers have to go to a prosecutor to obtain a warrant from a judge before accessing an IP, valuable time is lost operationally in disrupting cybercriminals (Interview, EC3 official, September 2014; see also UK-led cybercrime taskforce proving its worth, 2014). Another issue relates to information sharing – in particular with non-EU partners and private companies. Here, J-CAT is also developing an encryption system that will address issues of privacy, whilst also ensuring that information shared is specific to a particular task or case investigation (rather than exchanging bulk data). Whilst this is formative at best, if it is successful, it might well be diffused as a model of good practice across Europe and beyond (Ibid.), and go some way to addressing the balance between privacy and security – a debate exacerbated by the Snowden revelations in 2013, and in which the UK's GCHQ was implicated in collaborating to collect the data of citizens on a mass scale. Indeed although such collection of bulk data for security is controversial in the UK, the government has ensured the continuation of the practice through passing a new law

in July 2014 – the Data Retention and Investigatory Powers Act. This is despite the fact that such practice was rendered illegal by the decision of the European Court of Justice (ECJ) which declared the Data Retention Directive (2006) invalid in April 2014, precisely because it allowed excessive interference and violated citizens' rights to protect their data and privacy. There is then a tension in the UK that needs to be resolved between its national security logic[13] that drives such practice and its initiatives to create resilience through a broader set of cybersecurity objectives (see chapter 7).

Securing cyberspace for business: Partnerships, information sharing and standards

A major part of the UK's approach to cybersecurity is working with the private sector in order to raise standards, awareness and incentivise the sharing of information – all necessary conditions for effective security as resilience. With regards to the latter the main public-private platform (launched in March 2013) for achieving this is the Cyber Security Information Sharing Partnership (CISP). Now absorbed into and hosted by a new governmental institution, CERT-UK (which was established April 2014 – see below), it has exceeded its target of 500 members and aims to attract further members from across business, education and other sectors. The idea behind CISP is to provide a trust-based environment where government and industry can share data on cyber threats, incidents and vulnerabilities in real time. Information is provided by members and a fusion cell composed of industry and government network defence analysts examines the data and provides enriched data and advice to CISP members. Whilst initially technically focused, the broadening of membership has meant that CISP also provides more general information in order to raise awareness on cybersecurity issues.

The theory is that the CISP platform allows members to be more proactive in protecting against cyber threats – and build in the option of sharing publically or anonymously – the latter particularly important for those sceptical because of the potential economic impact of sharing information on incidents. Indeed CISP style nodes have been utilised for various events such as the NATO Summit in Cardiff (2014) and the Commonwealth Games in Glasgow (2014), and mirroring the ROCU model CISP nodes are also being rolled out regionally within the UK so that members can 'develop deeper trust relationships with partners they already know' (Gibson[14] cited in UK cyber threat sharing ahead of target, 2014). As we shall see in Chapter 5, familiarity and trust are key components in constructing effective, collaborative information sharing platforms and mechanisms.

This said, a potential issue that remains is how intelligence is shared and indeed in what direction. On the latter, certain commentators have noted the lack of intelligence flowing from GCHQ to industry[15] – and indeed argue that there is a need to integrate and improve mechanisms whereby information received by the intelligence services can be utilised and shared in real time to prevent and protect against cyber threats (Interview, Anonymous, August 2014). Indeed a survey published by InfoSec in 2014 found that 67% of information security professionals thought intelligence was not shared effectively between government and industry (cited in Update on the National Cyber Security Programme 2014, p.12). Furthermore, and this is acknowledged by the Director of CERT-UK, whilst the membership of CISP has risen exponentially, there is a long way to go with regard to the balance of membership – with SMEs in particular under-represented. Incentivising SMEs to collaborate will be critical if a more comprehensive approach to cybersecurity is to evolve in the UK.

Another key aspect of the UK governmental approach to create the market structures for effective security as resilience is that of incentivising the development of an industry-led organisational standard for business, in order to clarify what good practice looks like for companies and to also make this a differentiator in the market place. In this context the UK government has developed the 'Cyber Essentials' standard[16] which the Ministry of Defence requires its suppliers to meet as part of its standard contracting process. Indeed the aim of the UK government is to mandate this standard across government procurement where proportionate and relevant in order not to impose additional costs on businesses – in particular SMEs.

In addition to this, another UK incentive has been to develop, with the insurance industry, a UK cyber insurance market in order to drive improvements in cyber risk management. Whilst at the time of writing this has not been operationalised beyond agreement on broad objectives, it complements the overall hands-off governance approach of the UK government to incentivising industry and informing consumers alongside initiatives such as kite-marking and certification (of products, services and professionals), as well as guidance schemes (see Table 4.1) which seek to raise awareness and facilitate a movement towards a more effective security as resilience through changing the behaviour of cybersecurity stakeholders.

Specific guidance for different audiences has been a key lesson learnt by the UK government in the evolution of its cybersecurity strategy – with the initial feedback indicating that SMEs in particular needed more focused guidance that fit with their particular business models and

Table 4.1 Cybersecurity guidance for businesses

The 10 Steps to Cyber Security	Guidance for Chief Executives and board members on safeguarding their most valuable assets, including personal data, online services and intellectual property
Small businesses: what you need to know about cyber security	Guidance based on The 10 Steps, tailored for micro, small and medium-sized enterprises
Responsible for Information	E-learning for micro, small and medium sized businesses; FREE to access and role-based for employees, Information Asset Owners and Directors or business owners
Cyber Security for Legal and Accountancy Professionals	E-learning to help lawyers and accountants protect themselves, their clients and the sensitive information they hold on their clients' behalf
Cyber Security for Non-Executive Directors (NEDs)	Guidance to support NEDs who can advise companies on cyber security and encourage good management of cyber risks
Cyber Security in Corporate Finance	Guidance led by industry to help tackle cyber threats around mergers & acquisitions, buyouts and venture capital

Source: UKCSS: Report on Progress and Forward Plans, Cabinet Office (2014, p.4).

resource capability, and that government work to incentivise change in SME behaviour had the least impact compared to other stakeholders (Update on the National Cyber Security Programme 2014, p.15–16). Indeed the guidance for small business was updated (January 2015) and supplemented with the development, in partnership with industry, of a cyber action plan for small businesses, targeted advertising campaigns on information and guidance, and perhaps more innovatively, a cybersecurity Innovation Voucher Scheme worth £5000 to SMEs to incentivise them to invest in improving their cybersecurity and enhance growth potential (UKCSS: Report on Progress and Forward Plans, Cabinet Office December 2014, p.6).

With regards to standards – developing and incentivising the implementation of the Cyber Essentials standard does not ensure the adoption of that standard by all relevant stakeholders. This is especially true given the global nature of business and the availability of specific industry standards and regulations as well as other, international standards. This also then raises the issue of standards compatibility for global corporations that work across and within other jurisdictions

(Neville-Jones and Phillips 2012, p.39), although there is evidence of different standards organisations' collaborating together and with industry to resolve this issue to achieve some level of synergy and mutual recognition (EU NIS Cyber Security meeting, Brussels June 2014). Furthermore, and as certain industry representatives have noted, whilst the introduction of an industry-led standard is laudable – this is only a bare minimum and companies will have to do much more in order to ensure security of data and resilience (UK cyber security progress welcomed, 2013).

Finally, a key objective of the UK government in improving its cyber resilience is to maximise the opportunities this brings for exports in the UK cybersecurity sector and more specifically, to meet the Government target of increasing its share of the global market by £2 billion by 2016. To meet this objective the joint (government and industry) Cyber Growth Partnership was launched in conjunction with TechUK (which represents 850 UK technology organisations) which was also tasked with: promoting the Cyber Security Supplier to Government Scheme (CSSGS)[17]; coordinating export campaigns; and working with government to develop the provision of cybersecurity training and education in order to support the growth of the UK cybersecurity sector (The National Cyber Security Policy 2013, p.4).

Whilst it is too early at the time of writing to comprehensively assess the effectiveness of this Partnership, evidence suggests that those involved at the level of regional business clusters established and within the CSGSS (over 35 UK companies) are benefiting in terms of ideas for cybersecurity products, guidance and training. In addition, there has been a more inclusive approach from GCHQ with regard to involving SMEs in unclassified contracts, where they were previously excluded. Such an inclusive approach is important in resilience terms – and in particular given the criticisms from the National Audit Office (Update on the National Cyber Security Programme 2014, p. 17) that the UK Trade and Investment (UKTI) Department tasked with supporting cybersecurity trade and exports through its Defence and Security Organisation (DSO) has primarily focused on large deals with defence and maritime contractors and established companies. Beyond this, novel governance arrangements have been piloted in the form of an Innovation Centre in Gloucestershire to facilitate collaboration in research, experimentation and code development between staff and industry – and importantly, with plans to include SMEs and start-ups, and expand this to the national level (UKCSS: Report on Progress and Forward Plans, Cabinet Office December 2014, p.8–10).

Cyber-attacks and resilience

One dimension of the UK Government's objective to make the UK more resilient to cyber-attack has been to develop a new Public Sector Network (PSN) as a security model for sharing of services across public sector organisations; that is, to protect and make more resilient its own systems through establishing common standards, monitoring security and compliance and better network resilience. Whilst progress has been made in this dimension with all local authorities and Councils that are part of the PSN – this is not the case with all central government suppliers and departments – although the aim is for this and a compliance process validating appropriate technical and security standards to be rolled out across the PSN by the end of 2015. The UK government has also taken a number of measures – for instance GOV.UK Verify and other technical tools and advice – to ensure government online services are secure. It has also provided an e-learning course which has been completed by 500,000 public servants with additional face-to-face training for 3,600 staff for those in critical roles.

Several issues have been raised with regards to the UK government's approach to ensuring resilience of its own systems. The first relates to the impact of the training that has been completed and what effect this might have had on the culture of resilience among the staff that has undertaken it. Assessing the impact of the many government initiatives on cybersecurity has been a difficult exercise according to the National Audit Office (Update on the National Cyber Security Programme 2014, p.22–24) – but one that is essential in terms of the influence of training on the behaviour of staff and indeed users of government services if an effective culture of security is to evolve.

The second relates to the complexity of transition and the approach taken by the UK government with regards to integrating old and new systems, and in particular securing the government cloud. Specifically, Neville-Jones and Phillips (2012, p.36–37) have argued that the approach is underpinned by a perimeter security logic that is not alone, compatible with effective layered cybersecurity. They argue that there is a need for an even more comprehensive approach to cybersecurity, and more work is required to develop coherent security architectures that ensure tighter integration of software and hardware development at all stages within different layers. It could be argued that the government has gone some way to addressing such concerns through setting minimal standards for its own contracts where appropriate, providing incentives for industry to also adopt such standards, and launching Publicly Available Specification 754 (PAS 754) to codify what constitutes

good software engineering (for instance, to help organisations identify and employ trustworthy software)[18]; however, this does not imply that the approach could not be more comprehensive and coherent.

Finally, there is also an issue of resource with regards to system upgrades and transition to PSN as well as maintaining and upgrading measures and systems after transition. The Cabinet Office is unlikely to reveal levels of expenditure for cybersecurity beyond allocations for 2015–2016 before the UK general election in May 2015. If current levels of expenditure are not maintained this could mean that part of the transition burden would be covered after this period by departmental budgets. The effectiveness of the new system will then depend on cybersecurity remaining a priority across the public sector after this and indeed there being a fundamental transformation in the culture of cybersecurity to ensure that this happens, which is by no means certain. Additional resource beyond transition will be essential if the credibility and resilience of governmental systems are to be maintained beyond the life-cycle of the programme.

The second dimension relates to the protection and resilience of UK critical private sector infrastructure, in which the CPNI and CERT-UK formed in March 2014, play a critical role. Previous to this, as alluded to above, there was no single government CERT but rather two primary government CERTs that catered to different organisational groups: CSIRTUK, part of CPNI, that serves companies that make up the Critical National Infrastructure (CNI), and GovCertUK which provides response services to government and wider public sector organisations. In addition the MoD also has its own dedicated CERT (MODCERT) responsible for MoD networks (see Pritchard 2013). Furthermore, within the UK, ENISA's most recent report (2013) on CERT activity indicates that the UK has 22 public and private CERTs in total,[19] excluding CERT-UK.

Before 2007 CSIRTUK and GovCERT roles were combined in what in practice was a national UK CERT that was part of the predecessor to CPNI, the National Infrastructure Coordination Centre (NISCC), and which operated a Unified Incident Reporting and Alert Scheme – a central point for reporting incidents from the public and private sector (with an emphasis on critical infrastructure) and for producing alerts and information on cyber incidents and threats. This single point for reporting was lost when CPNI was formed even though the complexity of the cybersecurity threat increased exponentially in the intervening years; thus the UK system for reporting incidents remained fragmented, with CERT-UK aiming to fill this gap as the primary government CERT that is responsible for cyber incident management, handling

cyber incidents related to CNI, developing and sharing cyber threat situational awareness and providing an international point of contact on cybersecurity issues. This does not imply that the other existing CERTs in the UK will be dissolved, but rather that CERT-UK, as recommended and encouraged by ENISA, and for which it has defined minimum baseline requirements that such an organisation should meet, becomes the primary government CERT that, in theory, coordinates responses to cyber incidents.

From a security as resilience perspective CERT-UK, in principle at least, is an essential new institution that will facilitate more effective coordination to responses and information sharing internally within the UK, and externally in relation to providing a contact and liaison point for international partners on trans-border incident response. On the latter, it also ensures that trust is built through membership and regular contact with other CERTs around Europe through groups such as the Forum of Incident Response and Security Teams (FIRST) and the European Government CERTs (EGC). Building trust, as we shall also see in the coming chapters, is a critical element of building effective partnerships and in turn, security as resilience. This indicates that the UK understands and is willing to transform the way in which cyber incidents are dealt with rather than simply change policy at the margins.

However, and despite initial activity that indicates that it is fulfilling its role successfully – for instance, through providing information and advice on mitigation on the Heartbleed and Shellshock vulnerabilities, and working with CISP members to support the Commonwealth Games and NATO summit (see CERT-UK Quarterly Report 2014a, 2014b) – some have questioned the extent to which it adds value to what already exists and what is being done in the UK with regards to, for instance, situational awareness, incident management and threat analysis through the National Computing Centre (NCC) and CPNI and other CERTs (Jeffray 2014). Whilst specific Incident Report Guidelines set out and differentiate the roles of CERT-UK and GovCERT (Bada et al. 2014; CESG https://www.cesg.gov.uk), this is not the case across the board, and is an issue that will require more effective collaboration with the relevant sectors and existing CERTs in those sectors to avoid duplication and ensure coherence. Similarly, whilst many incidents are reported directly to CERT-UK from across various sectors – those reported through CISP are not included in the CERT-UK's statistical analysis of incidents, leading to an underrepresentation of certain sectors with regard to the types of incidents and challenges that they are facing, and thus understanding of what is at stake and appropriate incident response (through CISP

or CERT-UK). Further engagement with those sectors to improve knowledge of the issues they are facing then, will be critical moving forward if the conditions for effective cross-sectoral resilience are to emerge.

The third and final dimension is cybersecurity and defence, where the Defence Cyber Protection Partnership (DCPP) focusing on the supply chain was formed to play a similar role to CISP – to improve cooperation and information sharing between government and industry, and to focus on best practice, awareness and proportionate standards. The DCPP has also sought to move to more inclusive membership. Thus, as well as including major defence contractors (13 at the time of writing), trade associations such as ADS and TechUK which represent small businesses are also members. Whilst work is still formative within the DCPP, it has worked effectively with BIS and GCHQ to identify how Cyber Essentials can be implemented in the supply chain and additional controls (beyond Cyber Essentials) – technical (scanning for vulnerabilities, risk assessment), organisational (information security policy, roles and responsibilities), legal (compliance) and educational (people security/training) – that would need to be implemented by companies in the supply chain in a proportionate way. At the time of writing DCPP controls and standards are being piloted by the MoD – and if seen to be successful, will be mandated in MoD contracts from April 2015 (Defence Cyber Protection Partnership 2015), incentivising the adoption of such standards and controls whilst also ensuring that the conditions for convergence on common standards, controls and understandings of the cyber threat, and thus effective security as resilience, are being constructed.

Shaping the international

The global and borderless nature of cyberspace has meant that the UK government has had to think about and develop strategies to harness international partnerships of collaboration, coordination and cooperation in order to ensure security as resilience in the UK. This has taken the form of engagement bilaterally and multilaterally, shaping international debate through the 'London Process' and hosting international events on cyberspace, engaging in the development of norms of responsible state behaviour in cyberspace and capacity building, in order to ensure the inclusion of a broader range of countries and strengthen their abilities and knowledge in dealing with issues of cybersecurity.

A number of MoUs (Korea, Israel) and cyber dialogue (Singapore, Japan, China) agreements have been penned bilaterally, most interesting perhaps with regard to China – where an official dialogue channel exists

parallel to a think-tank led dialogue in order to improve understanding and indeed engagement with a key player in cyberspace. Further than this – and perhaps an example of good practice to be emulated through the EU if progress is to be made with countries with an alternative approach to cybersecurity (see Bersick et al. 2015) – the UK has also established a direct relationship between the UK NCA and Chinese law enforcement, establishing 24/7 contact points to fight cybercrime taking place between the two countries (Brewster 2014). Indeed such looser and less formal governance arrangements which have involved seminars in China for UK and Chinese cyber law enforcement agencies as well as visits to the NCA by the latter, might well be more fruitful in building trust and facilitating more effective collaboration and sharing of threat information.

Multilaterally, the UK has been involved in the shaping of the primary legislation that has emanated from the European Union (EU) on cybersecurity, and the EU's cybersecurity strategy that was published in February 2013 (see Chapters 5 and 6 for detailed analysis). Suffice it to say that the UK has sought to demonstrate its leadership in cybersecurity within the EU – and indeed to promote its approach to cybersecurity – that is, hands-off and meta-governance of identities – which has conflicted with the more hands-on approach in the proposed NIS Directive (see Chapter 6). Indeed the UK position on the content of the Directive has reflected its voluntary, market-based approach in its calls for reducing costs related to the proposed scope (including only critical infrastructure providers and not providers of information society services), and adding clarity to exactly how cooperation with regards to information sharing will work (Informal meeting, UKREP February 2014).

They have in particular been concerned about how trust can be built through imposition of reporting as opposed to informal arrangements that seek to establish familiarity and trust over time through developing effective working relationships. In this sense the UK and other EU member states with more mature and resilient levels of cybersecurity, have called for alternatives to mandatory reporting. Indeed the UK has stated a preference for 'two separate groups . . . one at technical/official level to get together to talk about implementation of the Directive . . . the strategic aspects of cyber security . . . and secondly, a group of member state CERTs getting together . . . on a voluntary basis . . . to start the process of information sharing . . . and developing a future roadmap for cooperation' (Telephone Interview, UK cybersecurity official, October 2014). Given the divisions with regard to the proposed NIS Directive and how

far it has already been watered down by various parties (see Chapters 6 and 7) it is clear that many more compromises will still need to be found if final agreement on its scope and content are to be arrived at. This is particularly salient from a UK perspective given its 'whole of business approach' to cybersecurity, and indeed for the rest of Europe in terms of the most effective way to construct the necessary conditions for achieving cybersecurity resilience.

The UK has also deepened its involvement in NATO through becoming a full member of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) and playing a prominent part in agreeing the Enhanced NATO Policy on Cyber Defence. Indeed the UK also proposed an initiative for a new partnership – the NATO Industry Cyber Partnership – aiming to ensure that expertise and innovation from the private sector is exploited as much as possible in order to achieve the objectives of the Enhanced Cyber Defence Policy. It is also clear here then – in cyber defence – that the UK has a preference for NATO as an intergovernmental organisation as opposed to the EU – as it has opted out of participating in the latter's efforts through the EDA on the grounds that 'cyber defence' is seen as a matter of national security and competence. Such logic, however, might well be counter-productive to achieving cybersecurity resilience in the UK and Europe – in particular given the shared interest and urgent need across the EU to enhance cyber defence capabilities and the blurring of the lines between military and private infrastructure for military operations.

Finally the UK has sought to shape the international norms for governing the Internet and state behaviour in cyberspace in order to create a shared understanding and promote a coherent approach to cyber threat beyond the UK. As discussed in Chapter 3, this is a difficult task given the conflicting or one might even say diametrically opposed views of key states and organisations. Whilst the UK has encouraged debate through conferences in London, Budapest and Seoul (via the London Process), this process, for some, has not amounted to any concrete agreement or consensus on the way forward; indeed, some have argued that these conferences have been no more than 'talking shops'. Beyond this, even where consensus seems to have been reached in terms of certain principles for governing behaviour through fora such as the UN Group of Governmental Experts (UNGGE) (that existing international law is applicable in cyberspace[20]); a consensus on broad norms and principles does not necessarily imply a shared understanding of Internet governance or cybersecurity, as shown in Chapter 3. The UK then is actively promoting the debate at international

level, including constructing confidence-building measures and guidelines through organisations such the OSCE and OECD, and encouraging increased participation through funding initiatives such as overseas scholarships for cybersecurity scholars, ICT4Peace and the Global Cyber Security Centre. However, much more thought must go into how such initiatives link with lower level informal interaction, cooperation and dialogue – as this is where changes in understanding through practice might well pay most dividend.

Knowledge, skills and capability

The UK is clearly one of the most mature EU member states with regards to education and skills initiatives to develop capability. The last two years have witnessed the construction of a comprehensive programme of initiatives (see Table 4.2) across industry and the academic sector to ensure that the requisite level of knowledge, skills and expertise is created to achieve security as resilience at different levels, including societal. This approach has involved targeted interventions in schools through to postgraduate education, with the help of expert groups (Tech Partnership, the British Computer Society, the Institute of Engineering and Technology, the Institute of Information Security Professionals and Cyber Security Challenge).

Despite this, however, it is clear that the cyber skills and education dimension in building resilience is both multifaceted and complex. Whilst initiatives (to name but two) such as the Cyber Security Challenge no doubt engage a broader pool of talent and Centres of Doctoral Training will no doubt produce skilled individuals in the medium to long term, there is a concern among certain stakeholders that the demand for technical skills in the short term will not be met, in particular in the public sector. The National Audit Office Report notes that 'the public sector is losing critical staff and there is an insufficient supply of professionals to replace them' (Update on the National Security Programme 2014, p.21). Although acknowledging that the cyber reservist initiative will help to build capacity in the MoD, the report also highlights that there remains a broader problem of recruiting and retaining experts and advisers across government that understand cybersecurity issues.

The UK thus is no doubt pursuing a multi-pronged approach to education and skills development in the UK, but with many of the benefits only likely to emerge in the medium to long term. There are certainly elements of good practice, however, that might be emulated elsewhere – but with the UK also able to improve on measures to train

Table 4.2 Cybersecurity knowledge, skills and capability

Schools	Learning and teaching materials at GCSE and A-level, new Key Stage 3 (age 11–14) materials to be released in 2015; now interventions at every level of the education system
Training and apprenticeships	200 new entry-level cyber security jobs through the Tech Partnership and employers, to add to 120+ GCHQ apprentices, plus a Cyber Intrusion Analyst Trailblazer Apprenticeship in 2015
Higher Education	4 Higher Education Academies to receive NCSP teaching development grants in universities, a mentoring scheme and 'Cyber Camps' for graduates and undergraduates
Postgraduates	GCHQ has certified six Master's degrees in General Cyber Security, plus 2 Centres of Doctoral Training to deliver 66 additional PhDs from 2017 on top of GCHQ's PhD programme
Wider educational support	Open University developed Massive Open Online Course 'Introduction to Cyber Security' – nearly 24,127 sign ups to the first offering, and a new App from GCHQ on coding, 'Cryptoy'
	GCHQ has recognised 11 Academic Centres of Excellence reflecting their high standard of cyber research
The Cyber Security Challenge	18,800 registered for the Masterclass competition; 800 schools participating in the Schools' competition; over 22,000 young people have used the learning resources

Source: UKCSS: Report on Progress and Forward Plans, Cabinet Office (2014, p.22).

and recruit in the short term on delivering, for example, on interdisciplinarity in cybersecurity education and training; the latter is not a unique UK issue, but one that exists across Europe and needs to be addressed if a more holistic understanding of cybersecurity issues and solutions to these is to evolve. Moreover, it is essential if a shared understanding of cyber threats is to evolve across the various layers and levels of cybersecurity, and therefore to the emergence of a culture of cybersecurity.

Finally the UK has invested in several initiatives and has provided several platforms for educating citizens and increasing their awareness of cyber threats. Building on the public-private sector 'Get Safe Online' scheme (launched in 2005) initiatives such as Cyber Streetwise

(launched in 2013) supported by a broad range of organisations (banks, BT, Facebook, Sophos, trade organisations), in its first phase, has according to the UK Home Office served to have a positive impact with regards to changing the practice of citizens. According to their figures, 65% of citizens now undertake at least ten out of the 17 recommended cybersecurity behaviours – for example, using stronger passwords or checking for certified signs for secure websites when shopping online (Update on the National Security Programme 2014, p.16). There is clear recognition that this is a starting point for raising public awareness and education in cybersecurity, and that in order to achieve a transformation in behaviour towards a culture of cybersecurity, more targeted and differentiated approaches would be needed for varied audiences and in particular the less ICT competent and those from lower socio-economic groups (The UK Cyber Security Strategy: Landscape Review 2013, p.28).

Conclusion: UK security as resilience

The UK government's approach to cybersecurity embeds within it a hands-off market logic of governance, which it aims to diffuse throughout and between the targeted pillars of its cybersecurity strategy utilising a variety of institutions, mechanisms and tools and importantly, involving a multitude of relevant stakeholders. In this context, much progress has been made in terms of putting into place the preconditions for an effective security as resilience to emerge – and the UK, in comparison to and alongside other EU member states, can consider itself to be advanced, at least in its initiatives and thinking on how to secure cyberspace.

In practice, the UK has demonstrated its preparedness to invest not just in terms of monetary resource, but also in the creation of new public sector networks and institutions, as well as agencies and platforms to combat cyber-attacks and cybercrime. Partnership has been placed front and centre of the UK approach – through CISP and CERT-UK or Cyber Streetwise, for example, domestically, and through formal and informal arrangements in terms of international engagement in order to create common understandings of cybersecurity – and establish standards that will allow a common culture of security resilience to develop in the UK, but also beyond. Indeed, much of the innovation in the UK approach provides food for thought for those across Europe that are less advanced in their cybersecurity preparedness.

This said it is also clear that the UKCSS is still in many ways formative in its implementation and its impact – given the diversity, newness and sheer number of its initiatives – it is difficult to assess accurately across the layers, levels and stakeholders that it aims to reach. There is still much work to be done within and across government – as well as between government and other stakeholders – before a common understanding of cybersecurity emerges with regards to threat and preventative and proactive solutions. From industry to individual level, whilst awareness and interest has demonstrably been raised – issues still remain with regard to improving cyber education, training and skills and creating a culture of cybersecurity that allows an integrated and more effective security as resilience to emerge in the short to medium term.

An essential part of this culture is building trust and information sharing, which from a UK perspective is best served by a voluntary approach. Here, there is a clear contradiction in logics with that embedded in the proposed EU NIS Directive – which argues for a mandatory approach. Going forward, any agreed compromise will no doubt create a tension between the EU and the UK approaches unless enough flexibility is created in the Directive to accommodate both logics. How this will play out in practice (implementation) might also be a cause for concern with regard to the impact on creating an effective culture of information sharing. Beyond this, it is essential that the UK continue to engage constructively within the EU on its cybersecurity strategy – which includes the defence dimension, if it wants to contribute effectively to the evolution of good practice beyond its borders in this realm, and ultimately, cyber defence capability in EU member states.

The UK, overall, is certainly progressing towards an ecosystem that speaks to integration with regards to its cybersecurity strategy; a challenge will be in sustaining momentum into the next cybersecurity programme cycle – which will ultimately depend on ensuring that at the very least, a minimum common understanding of the cybersecurity threat is diffused among all stakeholders that ensures effective partnerships, platforms, standards and skills continue to evolve. Moreover, the UK government will have to ensure that its many initiatives – and its hands-off approach – join up to provide for a coherent approach domestically; and internationally that its engagement allows both export of its own good practice (for example, J-CAT) (as well as import of good practice from elsewhere) and the evolution of iterative processes of learning that allow common understandings and effective practices – at least

at operational level if not normative level – to emerge with partners beyond the UK. It will also have to – GCHQ having been implicated in mass surveillance activities and creating vulnerabilities and backdoors to collect intelligence data – reconcile its approach to cyber defence and offence with the objective of achieving effective resilience in the UK (see Chapter 7).

5
The European Union and Cybercrime

Introduction

The European Union (EU) approach to cybersecurity has five priority areas (Cybersecurity Strategy 2013), and essentially three central strands. The first relates to protecting against and combating cybercrime. The second focuses on Network and Information Security (NIS), Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) and the third, less developed strand, on cyber defence. This chapter will focus on the former of these strands (Chapter 6 will focus on the latter two), although with the recognition that overlap does exist between them when analysing the security as resilience that underpins them within the EU institutional milieu. This is particularly important to be aware of in the context of the existing European Principles and Guidelines for Internet resilience and stability (2011) and the construction of a Cybersecurity Strategy for the European Union (EUCSS 2013). The EU institutional set up is still reflective of policy separation with DG Home leading on criminal law elements, DG Connect on network security and resilience, and cyber defence under the remit of the CSDP: the EU is, however, developing integrated working structures in order to facilitate a coherent approach to its cybersecurity strategy.

Cybercrime[1] in the global market has become a serious issue given the growth of the Internet and its importance to our economic and social lives. According to Eurostat (2010), 80% of young Europeans connect with each other through online social networks, and online e-commerce transactions total approximately $8 trillion. This increase in the use of the Internet has been accompanied by the proliferation of cybercrime activity – varying from identity theft, to selling stolen credit cards, to child sexual abuse. Reports have suggested that there are over

one million cybercrime victims per day worldwide (Norton Cybercrime Report 2013) and that the global cost of consumer cybercrime alone is approximately $113 billion – and the cost to Europe $12bn (Norton Cybercrime Report 2013) – with a suggestion that cybercrime is more profitable than the illegal drugs trade. Whilst any such figures and information on cybercrime must be treated with caution given the variance in which cybercrime is defined and therefore cost reported (not to mention the agenda of those doing the reporting), it is clearly an issue that has a damaging impact on citizens, governments and businesses in Europe; and an activity that is low-risk and highly profitable for cybercriminals. In short, it is an issue that if not addressed through an appropriate and effective security as resilience can severely hinder the EU's plans for economic growth embodied in the Europe 2020 strategy (2010) and the Digital Agenda for Europe (European Commission 2010; European Commission 2012).

Cybercrime policy within the EU has been driven and underpinned by its evolving Internal Security Strategy (2010), and externally by the European Convention on Cybercrime (2001) (hereafter referred to as the Budapest Convention). The Stockholm Programme (2010) setting out the European Union's priorities for developing an area of justice, freedom and security (2010–2014), has emphasised that EU member states should, as soon as possible, 'ratify the 2001 Council of Europe Convention on Cybercrime' seeing it as the 'central legal framework of reference for fighting cybercrime at global level'(2010, p.22). It also highlights a central role for the European law enforcement agency (EUROPOL), as a resource centre for Europe and the EU that can act as a platform for providing data and identifying offenders and offences, as well as assisting in the exchange of best practices between EU member states through communication and cooperation with national alert platforms. To this end, EC3 established on 1 January 2013, is seen as a central node in fighting cybercrime through pooling expertise and information, supporting criminal investigations, promoting EU-wide solutions, and raising awareness of cybercrime issues across the Union. Cybercrime and cybersecurity also figure high on the priority list of the next programme – the Rome Programme (2015–2019). Indeed the UK's House of Lords review of the Stockholm Programme has recognised that cybercrime and cybersecurity would require further attention during the life time of the new programme – and have in particular recommended a more strategic approach and emphasised the need for closer cooperation between the public and private sector (House of Lords, EU Committee 13th Report 2014, p.16–17).

Beyond this, the EU has developed a series of other initiatives that seek to address the issue of cybercrime across its different dimensions. This includes, for example, the Directive on combating the sexual exploitation of children online and child pornography (2011), as well as a Directive on attacks against information systems with a focus on penalising the exploitation of cybercrime tools, in particular botnets[2] (2010). Cybercrime remains a top political priority for the EU and is one of the eight priorities of the EU policy cycle for organised and serious international crime. According to the European Commission (2012, p.3), 'it forms an integral part of efforts to develop an overarching EU strategy to strengthen cyber-security'. The EU has, clearly, recognising the global nature of the cybercrime threat, also sought to engage with international partners, with the EU–US working group in cybersecurity and cybercrime of primary importance (see Chapter 7). Among the key objectives of the partnership are to advance the Budapest Convention (2001) and to increase public-private partnerships for the purpose of sharing best practices on issues such as botnets. The latter objective of creating and enhancing public-private partnerships is also spelt out in the Stockholm Programme (2010, p.23), as is clarifying legal rules that promote cooperation in cross-border investigations into cybercrimes. Finally the EUCSS (2013, p.9–11) details further how the EU plans to facilitate movement to enhanced capability to combat cybercrime and improve coordination between key actors in Europe and globally.

Many of the initiatives outlined above, including the creation of EC3, have been triggered by obstacles that continue to exist for dealing with cybercrime effectively, including: 'jurisdictional boundaries, insufficient intelligence-sharing capabilities, technical difficulties in tracing the origins of cybercrime perpetrators, disparate investigative and forensic capacities, scarcity of trained staff, and inconsistent cooperation with other stakeholders responsible for cyber-security' (European Commission 2012, p.3). This chapter will aim to assess the extent to which the EU is meeting its objectives with regard to the ecosystem under construction for cybercrime, and importantly, how far such objectives deliver on removing such obstacles and constructing the necessary conditions for effective security as resilience across the different dimensions – legal, economic, political, cultural, operational and strategic – of cybercrime. It will be structured as follows in order to achieve its aim. The first section will provide a context within which to understand the evolution of cybercrime policy within the EU, and a critical analysis and assessment of its approach to security governance in cybercrime. The second section will evaluate how the EU is contributing to and

promoting approaches to cybercrime, with a particular focus on the proposed measures of the EUCSS (2013).[3] The final, concluding section will then evaluate the progress the EU is making in the construction of an effective security as resilience for Europe, and the challenges that remain in practice.

Governing cybercrime in the European Union

EU approaches towards cybercrime have developed in parallel to its information society strategies such as the *e*Europe (European Commission 1999) initiative for enhancing the use and enjoying the benefits of digital technologies in a socially inclusive way. As the EU's aspirations to become an information society have progressed, so too have its efforts to protect those emerging benefits from criminal activity. In this context the *e*Europe initiative was followed by an *e*Europe Action Plan agreed in June 2000 at the Feira European Council, which emphasised the salience of addressing issues of network security and combating cybercrime. More specifically, the proposed approaches at this stage were both of a policy and a technical nature. For enhancing Internet security, whilst acknowledging that industry was primarily responsible for this (European Commission 1999, p.11), it also argued for the evolution of a public-private relationship for nascent industry, whereby the public sector was seen as playing a catalysing, stimulating role for private initiatives. There was a clear steer towards a hands-off meta-governance approach to reinforce private sector driven action. There was also an emphasis in the Action Plan on developing better co-operation and co-ordination related to the discussion of the Budapest Convention in different international fora. In terms of a the technical layer, the increased use of smart cards was proposed, 'as an enabling technology which can increase the level of confidentiality and privacy in information society services' (Ibid.) (for example, SIM, wire/contactless, embedded and wearable devices with multiple functionalities – access, identification, authentication and so on). The smart card initiative was backed with €100m research funding, and culminated in a smart card charter that was launched in December 2002.

The final report on *e*Europe (2003) noted some progress on the issue of Internet security, but also that use of the Directives launched (Electronic Signatures,[4] 2001) remained limited. However, *e*Europe did provide the basis for a more comprehensive approach to network and information security by the EU. In June 2001, two parallel documents were published by the European Commission that outlined the contours

of this comprehensive approach that also aimed to address crime in cyberspace. The first of these, a communication (European Commission 2001a) entitled 'Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-Related Crime', proposed a series of substantial and procedural legal provisions, as well as non-legal measures to address the criminal activities domestically and transnationally, whilst also stressing the need to preserve the balance between security and respect for the fundamental rights of individuals (2001a, p.2).

In terms of substantive law, for instance, there was an emphasis on agreeing on common definitions of cybercrime, as well as common incriminations and sanctions and introducing EU enforcement mechanisms that build on the Budapest Convention to enable it to take effective action on issues such as child pornography, racism and xenophobia online (Ibid., p.14–15). Procedurally, the central focus was on criminal law and the steer was on the improved cooperation of law and other enforcement agencies (through mutual recognition but also enhanced mechanisms), in line with EU law, to facilitate more effective responses and requests from other countries in relation to cybercrime offences (Ibid., p.16–24). A critical security governance dimension here was cooperation at the international level, and clear rules on transborder search and seizure. Finally, the non-legislative element focused on practical measures – or conditions – very much in line with the G8, ten point action plan (see Chapter 3) which in terms of broad themes, included: creating specialised cybercrime police units at national level (with law enforcement and judiciary personnel) where they did not exist; improved cooperation between stakeholders, that is law enforcement agencies, industry, consumer representatives and data protection authorities; and encouraging appropriate industry and community-led initiatives. Within these themes, and connected to the technical and policy layer, was incorporated attention to the liberalisation of encryption tools within the remit of community law, and the development of technical expertise and training, common rules for keeping records and information (for the purpose of information sharing), cooperation between EU actors and action from industry, in particular through research and development (Ibid., p.24).

The second, a proposal entitled, 'Communication on Network and Information Security: Proposal for a European Policy Approach', (European Commission 2001b) focused on issues such as identity theft, cyber and infrastructure attacks and provided recommendations on how to enhance security as resilience within the technical, legal and policy

layer. It was also underpinned by the security governance logic that 'market forces do not drive sufficient investment into security technology or security practice' and thus that 'policy measures can reinforce the market process and at the same time improve the functioning of the legal framework' (2001b, p.14). There was a clear indication then of a move away from the meta-governance of identities to hands-off (facilitation, incentives) and hands-on methods of security governance (legal framework), in order to secure the internal market for information and communications services and 'benefit from common solutions' as well as being able 'to act effectively at global level' (Ibid., p.15).

The central proposed tools or actions included: awareness raising and educational measures for all stakeholders; sharing best practices in security between member states; and the enhancement of cooperation between computer emergency response teams (CERTs) in Europe in order to ensure that information on potential and imminent threats is being exchanged, effectively. In addition, there was a strong steer towards 'strengthening the public/private cooperation on dependability of information infrastructures' (Ibid., p.17) in the context of the *e*Europe Action Plan; investment in network and information security which was considered to be sub-optimal, and specifically, in order to facilitate this, the inclusion of security in the Commission framework research programmes; ensuring the interoperability of security – enhancing solutions through standardisation and certification (that is, ensuring the use of standards that can be implemented across platforms) through supporting user-friendly solutions, stimulating internationally agreed standards, and encouraging participation of stakeholders in European and international standardisation organisations and activities (European Committee for Electrotechnical Standardization (Cenelec), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C)); legal measures[5] that sought to approximate national criminal laws related to cybercrime and security, as well as efforts to develop a common understanding of the legal implications of security in electronic communications and support for access to encryption products throughout Europe; finally, there was also an emphasis, given the borderless nature of cybercrime and security, on continuing efforts to support and contribute to the development of international efforts to combat cybercrime and security (Ibid., p.17–22).

Building on the above the EU sought to enhance its comprehensive approach through various framework decisions and communications. The framework decision on attacks against information systems

(Council Framework decision 2005/222/JHA, p.1), in essence, provided for a more robust legal layer or environment for prosecution and aimed specifically to 'improve cooperation between judicial and other competent authorities . . . through approximating rules on criminal law in the member states'. This framework decision provided common definitions for cyber-attacks with agreement on definitions by member states on what constituted criminal activity, which included: 'Illegal access to information systems', 'Illegal system interference' and 'Illegal data interference'[6] (Ibid., p.2–3). With a similar aim of moving to a common legal environment on the issue of sexual exploitation of children and child pornography a separate Council framework decision was agreed (2004/68/JHA), which included provisions to prevent the exchange of child pornography over the Internet. This framework decision, however, stipulated only minimal requirements in terms of approximation of legislation across member states, and subsequently led to problems in prosecuting offenders, within and between national borders. The security as resilience logic behind these framework decisions though was to make cooperation and coordination of efforts easier among the relevant public authorities, even if in practice there remained constraints given that there was no real culture of security that underpinned them.

Such a lack of 'culture' was highlighted in a communication from the European Commission outlining a 'Strategy for a Secure Information Society' (2006), and following the launch of 'i2010 – A European Information Society for Growth and Employment' which underlined the reliability and security of networks and information systems (European Commission 2005) for society and economy. More specifically, this communication aimed to 'develop a dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnership and empowerment' (2006, p.3). The Commission recognised that it had to achieve convergence and coherence on the hitherto multi-pronged approach to ensuring the security of the Information Society, which consisted of the fight against cybercrime, but also specific network and information security measures and a regulatory framework for electronic communications that addressed the issues of privacy and data protection.

Indeed, despite previous efforts to address the issue of cybercrime not only at European, but also at international and national levels, several key challenges remained that would require further regulatory and policy attention. The first was the motive for cybercrime, which had switched from simple disruption to the desire to make profit. This had seen the proliferation of a number of malware vehicles for

cybercriminals to achieve their aims, including spam, spyware and phishing, with an increasing reliability of compromised servers and computers for their distribution (2006, p.4). Mobile telephony (mobile based network services) and 'ambient intelligence' (intelligent devices supported by computer and network technology) constituted other challenges to the integrity and security of the Internet, as platforms that opened up new opportunities for attack by cybercriminals. Significant here was that the approach advocated by the Commission indicated more explicitly a movement towards a 'holistic approach' that chimed with an open, adaptable and inclusive resilience, through hands-off (supporting partnership, coordination) and hands-on (legislation to add legal clarity and improve cooperation between law enforcement agencies)[7] meta-governance. Moreover, it demonstrated an understanding that a multi-stakeholder approach and improved knowledge of the problems would be required if a culture of cybersecurity was going to emerge that was more likely to deal not just with the symptoms, but also the underlying causes of cybersecurity problems, at individual and institutional levels (public and private).

The Commission also indicated in this document that such an approach would complement its activity for protecting CIP, for which ENISA established in 2004 would play a key role in identifying best practice, improving awareness, and cultivating trusted partnership among all stakeholders (Ibid., p.6–9). More specifically, ENISA was also tasked in its original mandate (2005) with supporting national CERTs, for which it established a CERT programme and Working Group on CERT Co-operation and Support. This work included the identification of broad baseline capabilities, and gap analysis in the area of operational considerations and legal and regulatory factors, and has involved more recently (see below) work on good practice in relation to the network and information security aspects of cybercrime (ENISA 2012).

Clearly then, even at this early stage, the EU, at least in its official documentation and discourse, recognised the conditions necessary for an effective security as resilience to emerge. The hands-on meta-governance dimension was further developed in the Commission's communication 'Towards a general policy on the fight against cybercrime' (European Commission 2007) where it sought to improve cooperation and coordination at an operational and strategic level among law enforcement agencies, and at a political level among member states of the EU. In addition it promoted cooperation, legal and political, with third countries, and it put a specific emphasis, in the context of an evolving security as resilience, on continuous learning – through articulation

of training needs in relation to cybercrime issues for law enforcement and judicial authorities, and indeed, increased linkage and commonality between the training programmes of the authorities involved in order to achieve better coordination.

Furthermore, and given the important role of the private sector in any effective security as resilience solutions, the improvement of the public-private aspect of the Commission's cybercrime policy through enhanced mechanisms of dialogue was emphasised.[8] Examples of good practice in this sense included efforts to combat child pornography, where effective collaboration between credit card companies and law enforcement agencies assisted police in tracking down those that purchased online child pornography, as well as structures such as the Fraud Prevention Expert Group. Despite this, the challenge was to improve operational cooperation in Europe given the lack of legal obligation for private companies to share information on cybercrime with public authorities and the economic logic within which the former operated that prioritised the business model, and therefore secrecy rather than open sharing of information that might threaten reputation and profit (Interview, ENISA, July 2012).

Integral to improving cross-sectoral exchange of information, a crucial condition for security as resilience, was also the EU's rules on data privacy, retention and protection of personal data. The Directive on Data Retention (2006)[9] is particularly salient here in achieving an information-sharing culture and integrated framework and approach, as there was a requirement within it for all member states to put legislation in place that ensured ISPs and telecommunications companies maintained records on user traffic (connections not content) for between six months and two years. Whilst this was already established practice for many telecommunications companies, this was not the case for many ISPs – and added to this was the many technical and legal differences in national provision on data retention, which made measures to combat cybercrime largely ineffective, technically and at policy level.

This Directive sought to remedy this situation, although not without controversy, as many digital rights groups have been critical of the lack of transparency with regard to the use of collected data and the potential for its misuse.[10] The European Parliament has also argued that it fosters a surveillance society and undermines fundamental rights. Moreover, the Directive whilst transposed in the majority of member states has been the subject of legal challenge at national and European level (ECJ) – and the Commission's report on the evaluation of the Directive (2011) revealed that there were many inconsistencies in the way in which it

was implemented and which authorities were able to access the data. In addition, the European Data Protection Supervisor (EDPS) argued that the European Commission has not proved that the Directive is necessary and proportionate, which would make it illegal under the EU Charter of Fundamental Rights constituted by the Lisbon Treaty (European Frontier Foundation 2011).

There is then a real tension between ensuring access for security, and preserving the privacy of personal data, which is embedded not just in the legal, but also the political and cultural dimension of achieving a politics of resilience. The European Commission in its review of data protection rules carried out over the last few years, although reinforcing that the core principles underpinning its approach (from the original 1995 Directive) are still valid – to protect people's fundamental rights and freedoms, including data protection, whilst ensuring a free flow of data – acknowledge that modern technology throws up new challenges with regard to ensuring the highest standards for data protection within the EU and globally. However, it has not yet diffused the tension between security and rights; indeed, the exposure of the PRISM programme by Edward Snowden in 2013 only served to exacerbate this tension – with implications across the different levels and layers of cybercrime (see Chapter 7 for more detail). Even prior to the Snowden revelations there was a great degree of scepticism with regard to the balance between security and privacy for individuals,[11] with civil society groups asking for further oversight on the impact of the Directive on citizen privacy and evidence to suggest that it cannot be designed in a less privacy-intrusive way in the future. A shadow evaluation report by European Digital Rights (April 2011, p.20) concluded that

> the evaluation report of the Commission and the shadow report of European Digital Rights show that the Directive has failed on every level. It has failed to respect the fundamental rights of European citizens, it has failed to harmonise the Single Market and has proven unnecessary to fight serious crime.

The European Commission has recognised, in the past, the complexity of achieving balance through its actions, and has often taken the pragmatic view that the right to anonymity (privacy) and accountability (access) are not mutually exclusive when it comes to online crime (Interview, DG Home, November 2011). For example, such an approach was embedded in the proposal for 'A comprehensive approach on personal data protection in the European Union' (2010, p.14) which argues that

there is 'a need to consider the extent to which the exercise of certain data protection rights by an individual would jeopardise the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in a specific case' and that this might very well 'directly affect the possibilities for individuals to exercise their data protection rights in this area' (Ibid.).

The new proposed comprehensive 'legal' framework then, would not replace sector-specific legal instruments in the area of police and judicial cooperation in criminal matters that govern the functioning of agencies such as Europol[12] and Eurojust. These agencies either operate under their own specific data protection regimes or, more usually, utilise data protection instruments at the Council of Europe. The task for the EU then – in particular given that the Data Retention Directive was declared invalid by a European Court of Justice decision in April 2014 ruling that it represented an infringement on the individual's right to privacy and protection of data – is to align the specific data protection rules with the more general legal data protection framework, and more broadly, to demonstrate that targeted 'harmonised limitations' to certain data protection rules are beneficial to securing the very rights and freedoms that individuals enjoy online. This is no easy task given the broad debate on privacy and security, and the many different interpretations of EU rules on data protection by stakeholders, including National Data Protection Authorities. In resilient security governance terms, there is no uniform interpretation, application, or implementation of such rules, thus making it much more difficult to ensure effective cooperation and coordination with regard to cybercrime.

The Regulation (General EU Framework for Data Protection)[13] and Directive (on protection of personal data related to criminal and judicial activities)[14] that were produced in 2012,[15] sought to navigate through these issues for the purpose of achieving a more coherent and comprehensive approach to data protection. The new framework (Regulation and Directive) is a clear step change with regards to further hands-on meta-governance in this area. The Regulation seeks to introduce further rights for individuals concerned with disclosing personal data online and to create legal certainty for business, whilst the Directive is intended to clarify the relationship between the protection of personal data and the processing of personal data for police and criminal justice cooperation. Although the latter was previously covered by a framework decision (2008/977/JHA), it did not provide the EU with the power of enforcement, and was limited to cross-border processing activities, which caused significant practical difficulties in implementation

due to the confusion over when and how domestic data could be included, processed and used in any investigation (see Implementation Report on the Framework Decision (COM (2012)12)). In theory then, this new framework will facilitate the emergence of certain key conditions for an effective security as resilience to emerge in this area through enhancing trust between the transnational actors involved (police and judiciary), whilst also improving cooperation and smoother cross-border exchange of data in cybercrime investigations. Specifically, for example, both the Directive and the Regulation may be beneficial to certain CERTs and law enforcement agencies (LEAs) with regard to setting common ground rules that would help to legitimise their activities in relation to cybercrime investigations and incidents (ENISA, 2012b, p.52). It remains to be seen in practice, however, how far the logics and specific measures within the overall framework integrate satisfactorily the notions of privacy and security, in particular as according to certain commentators this legislation is still underpinned by 'a classical security vision, and an opposition of rights and security' (Porcedda 2012, p.71).[16]

Exploitation of the online world for the purposes of abusing children

One of the growing problems in relation to cybercrime given developments in the IT environment and the increased use of the Internet more generally across different dimensions is the exploitation of the online world for the purposes of abusing children. Whilst the EU has had legislation in place since 2004 to address the issue of sexual abuse and exploitation of children and child pornography,[17] this legislation was reconsidered precisely because of such new developments and the opportunities that this brought to criminals. The 2004 framework decision was deemed inadequate in several ways, not least because it only introduced minimal approximation of legislation in member states, which made it difficult for national authorities and agencies to coordinate and cooperate in investigations. In addition, given that it had been operational since 2004, new forms of sexual abuse and exploitation facilitated by the Internet (for example, grooming and pornography) were not criminalised. The revised proposal submitted by the Commission in 2010 (and agreed in June 2011) sought to move beyond minimal legislation to a more hands-on meta-governance in terms of scope and substance – in criminalisation of child sexual abuse and exploitation (substantive criminal law), cross-jurisdictional investigations, proceedings, and cases, and the prevention of offences, such as,

for example, national mechanisms to block access to websites with child pornography.

This latter aspect has not been without its controversy as it once again played into the debate on digital and human rights, and had implications for the type of governance required for effective security of resilience in cybercrime. In essence, the original proposal by the Commission suggested 'a mandatory blocking of child pornography', that is, a more direct role for government in such matters (Interview, DG Home, November 2011). A subsequent draft also placed more of an emphasis on empowering police and judicial authorities to enforce blocking of pornographic content, that is, a move away from judicial takedown (European Parliament, Draft Report January 2011) and what certain lobbyists have labelled 'Internal Self-Regulation', to a more delegated hands-on form of governance or what some have labelled 'External Self-Regulation' or devolved enforcement (European Digital Rights 2011, p.6). The European Parliament rejected the original proposal for mandatory blocking, and the compromise text provided a governance choice in transposition in that '*Member States may proceed with the means they consider most appropriate for an immediate intervention to stop further viewing and downloading of the image to prevent further damages to the victim'* (European Parliament, Draft Report January 2011, p.14). The implication here then, is that different actors are driven by fundamentally different logics when it comes to the issue of effectiveness in tackling cybercrime. This is just one example of the tension that exists between the legal, regulatory and policy layers, but which also has implications for what can be used within the technical layer in order to combat the exploitation and abuse of children online (for example, the use of surveillance and tracking technology).

Connected to the general objectives of the Action Plan to implement a concerted strategy to combat cybercrime (2010) concerning the improvement of trust, cooperation and coordination between public and private actors, further initiatives have been launched in order to deal with child abuse online within and beyond Europe. For example, as part of the Safer Internet Programme,[18] the European Commission is a central node that supports a network of non-governmental organisation (NGO) run hotlines in EU member states that collects reports on child abuse websites so that they can be removed and investigated. Child abuse content related to online offences is mainly dealt with by Europol, but the Commission also supports initiatives such as the European Financial Coalition (EFC),[19] made up of ISPs, banks and payment system suppliers, NGOs, telecom companies as well as

agencies such as Europol, Eurojust and police and judicial authorities in Europe (for examples, see The Digital Economy 2014). At the global level, and with similar operational aims to the general Action Plan in terms of improving the legal framework, joint cooperation across jurisdictions, education, and further encouraging the role of the private sector, the Global Alliance against Child Sexual Abuse online was launched in December 2012. In essence this Alliance will operate through an Open Method of Coordination (OMC) mode, with the objective of sharing best practices through regular reporting. Whilst such initiatives certainly speak to improving not just the European but global ecosystem for combating cybercrime in the medium term, it is much too early to assess how effective this will be in practice, although preliminary reports suggest both progress and obstacles with regard to the agreed four core policy targets (Report of the Global Alliance 2013; see Chapter 7 for more detail on this EU–US joint initiative).

Finally, DG Connect (formerly Information Society) has also sought to enhance a culture of security – at the level of the individual and collective – through its flagship initiative European Strategy for a Better Internet for Children (2012). It is underpinned by the concern for enhancing security through 'stimulating the production of creative and educational online content for children', awareness raising and teaching of online safety in all EU schools to develop children's digital and media literacy and self-responsibility online; creating a safe environment for children where parents and children are given the tools necessary for ensuring their protection online – such as easy-to-use mechanisms to report harmful content and conduct online, transparent default age-appropriate privacy settings or user-friendly parental controls; and combating child sexual abuse material online by promoting research into, and use of innovative technical solutions by police investigations'.

Preliminary assessments of how far progress has been made on realising the above four pillars of the strategy – and thus several of the conditions for the emergence of effective security as resilience – are few and far between given that it was only launched in May 2012, but those that do exist suggest a mixed picture. In the UK, for example, a study suggests (Livingstone 2013) that whilst there is a generally positive evaluation of available high quality content for children (56% of children in the UK say it is 'very true' compared to a European average of 44% with regards to what 'good' things are available for them online), the story is less positive with regards to awareness and empowerment, where there

has been little change across a range of key indicators since the launch of the strategy. To elaborate on this, 'one third of 12–15 year olds do not check the reliability of new websites they use (a figure that has barely changed over the past six years)' and a study by *EU Kids online* (2010) also found that

> only 59% of UK 11–6 year olds can change their social networking privacy settings and only 58% say they can judge the validity of websites. Meanwhile, half (51%) say they have spent less time with family and friends than they should because of time they spend on the internet (much higher than the 35% European average).

On awareness-raising, whilst there is evidence of good practice coming from industry and NGOs, assessment of impact is non-existent and the government resource has been cut in this area.[20] Such issues, of course, are only indicative of some of the broader challenges for creating a more effective culture of security across Europe and globally, but demonstrate that considerable barriers do exist to fulfilling any such condition in the short term, in particular if the resource required is not made available.

The cybersecurity strategy of the European Union: Cybercrime

Whilst the E-Privacy Directive (2009) prohibited the practice of infecting computers and turning them into botnets, technological developments and the increased use of sophisticated attack methods by criminals highlighted the need for further action in order to combat this growing threat. The Directive on attacks against information systems (2010) built on a review of the implementation[21] of its predecessor,[22] and identified, among other things, the lack of harmonisation in the legal framework of the EU as a major obstacle to effective security as resilience in cybercrime. Indeed it represented a step-change within the governance of combating cybercrime and in particular the use of botnets. Whilst this Directive was proposed in 2010 its agreement was delayed significantly by internal disputes between the Council and the European Parliament over Schengen, eventually being adopted by the parliament on 4 July 2013, with the following general aims:

1. To move towards more uniform criminal procedures and law in relation to criminal attacks on information systems across member states

2. To foster and improve coordination, cooperation and information exchange among the relevant actors across the EU member states and between EU agencies, EU member state agencies and relevant international bodies
3. To facilitate cooperation between and within public authorities, the private sector and civil society

The EU approach to cybercrime is fragmented, in the sense that there is no overarching framework but rather a series of legal and regulatory instruments that overlap, as demonstrated in the above analysis. Indeed, whilst a more comprehensive approach to cybercrime was considered an option by the EU, as was updating the Budapest Convention in the impact assessment for the Directive on attacks against information systems (2010), these were not deemed viable. Instead the EU moved to define a strategy – articulated first in a proposal for Internet security (2011) and then in a more elaborate form in the EUCSS (2013), with five clear priorities, one of which is 'drastically reducing cybercrime'. Within this priority there is a focus on the legal dimension – national, regional and global – as well as the operational layer and coordination between and within all levels relating to cybercrime.

These different elements speak directly to the preconditions necessary – in the legal and operational layers primarily – for an effective security as resilience to emerge (see Table 5.1), and in particular to the

Table 5.1 European Union cybercrime governance

Dimensions	**Main Actors/Institutions**
Legal	DG Home/DG Justice National governments Council of Europe (Budapest Convention)
Operational (& Technical)	EUROPOL/European Cybercrime Centre (EC3) International/National Cybercrime Units and Agencies EUROJUST European Police College (CEPOL)
Coordination and Information Sharing	EUROPOL(EC3)/ENISA/EUROJUST/CEPOL International/National Cybercrime Units and Agencies Transnational Networks/Initiatives Private sector/Industry

criterion of creating a culture of cybersecurity within and between different dimensions of the emerging cybersecurity ecosystem. The remainder of this section will analyse the progress that has been made in practice with regard to the objectives highlighted in the Cybersecurity Strategy[23] and highlight the potential obstacles that stand in the way of progress towards effective security as resilience as well as opportunities for progressing towards its achievement in relation to the EU's emerging system.

Legal

Within the legal dimension there is an emphasis, first and foremost, on signing, ratifying and implementing the Budapest Convention to ensure a common legislative platform for fighting cybercrime (see Chapter 3). The Budapest Convention was drafted precisely because of the difficulties in regulating and governing cybercrime, in particular in relation to issues of defining cybercrime, defining common standards for addressing and preventing cybercrime and a framework for cooperation, evidence collection and prosecution among the relevant law enforcement agencies.[24] However, whilst much progress has been made within the EU by the Commission, and externally, by the EEAS, to promote the convention as the main instrument of choice and indeed model for fighting cybercrime at EU member state (national) level, only 24 out of the 28 EU states have ratified it.[25] The reasons for this have varied, from: political motivation and disagreement based on freedom of expression online, principles of data handling and protection; to a lack of institutional and human capacity (skills) at national level; to arguments about the dynamism of the convention and differences in legal interpretation and culture, leading to asymmetric implementation, for example, data sharing and retention legislation (Yannakogeorgos and Lowther 2013, p.253). Some, for example, such as Ireland, signed the convention in 2002, but have failed to bring in any legislation to allow its ratification. In this sense then it seems that certain countries within and outside of Europe have 'ceremonially signed' the convention but 'it has not been fully accepted' (Hilley 2005, p.171); indeed even where implemented, different interpretations of cybercrime have not led to harmonised legal rules or cultural convergence on how cybercrime should be dealt with.

Whatever the reasons might be, the fact that not all EU member states have ratified and implemented the convention (it is not mandatory) hampers efforts to construct an effective security as resilience which relies on building trust, sharing information and intelligence, and cooperation and engagement between public and private actors involved in

gathering evidence and prosecuting online criminals. Moreover, it hinders convergence towards a common definition and understanding of cybercrime and the necessary procedures to ensure effective cross-border law enforcement to deny safe havens to cyber criminals. Furthermore, if there is no appropriate common or harmonised procedural and legal framework across the EU and indeed globally, it can hinder in a very practical way – policy coordination and prosecution. If there is no standard agreement on what data can be shared on cyber criminals, how evidence can be collected and used, and at a base level what constitutes cybercrime in different countries of the EU, then this erects very real barriers to creating a security as resilience among the relevant actors. This is not to suggest that if all EU member states ratified and implemented the convention that this would be a panacea – cybercrime is a global problem, and the convention has been extensively criticised with regard to the limitations in its provisions and because it represents an exercise in 'symbolic legislation' (Marion 2010, p.699) rather than a genuine attempt to address the legal issues raised by international cybercrime and criminals. For instance, the convention does not provide rules on the safe storage of seized information whilst investigations are being conducted, implying that information legally stored by a CERT in one member state, may not satisfy legal requirements in another member state. This in turn has implications for what sort of information can be considered as evidence in the investigation of cybercrime and the prosecution of cyber criminals (ENISA, A Flair for Sharing 2011, p.39).

Limitations aside, and as one senior DG Home official recognises in the context of the EU's strategy for promoting it beyond its borders, 'it is difficult to push the Convention outside if all our Member States have not ratified it....' (Interview, DG Home, March 2013). Thus its ratification and implementation within the EU would at the very least, ensure that there is a platform for a culture of cybersecurity to emerge based on a common (not necessarily completely harmonised) framework and an integrated approach; pre-requisites for constructing an ecosystem that embeds security as resilience across and between layers and levels. It would also provide the EU with greater credibility in its arguments to persuade those outside the EU to sign and ratify the convention. This is not to say that the convention itself is the perfect instrument in such an ecosystem, as noted above – but it is certainly more adaptable and flexible than many critics suggest – and represents good practice across the different dimensions of the fight against cybercrime. Thus whilst the ratification and implementation of the Budapest Convention

certainly remains problematic from a security as resilience perspective – within the EU and globally – it at least provides a basic platform for constructing the necessary conditions to be more effective – in particular in relation to cooperation – whether this is between public-private actors, political decision-makers, international organisations, or technical and legal professionals.

The other main legal aspects that actually emanate from within the EU are the Directive on combating the sexual abuse and sexual exploitation of children (European Parliament and the Council 2011/93/EU) and the Directive on attacks against information systems (European Parliament and the Council 2013/40/EU). The former has been dealt with in detail in the section above, and the issue of transposition and compliance with it by EU member states is, at the time of writing, being assessed by the European Commission. The latter will not be implemented into national law until 4 September 2015. Both Directives are being evaluated by the Council General Secretariat after the selection of cybercrime as the subject for the seventh Mutual Evaluation round, which will look specifically at the practical implementation of EU policies on cybercrime in three specific areas: cyber-attacks, child sexual abuse/pornography online and online card fraud, in order to shed light on legal and operational aspects as well as issues of cross-border cooperation and coordination between and within relevant national, EU and international agencies (Council of the EU, REV1, Limite, GENVAL 3, CYBER3).

Cooperation, collaboration and operational aspects

The EU cybersecurity strategy highlights the issue of coordination and collaboration, in particular with regard to bringing together the different stakeholders that must work together in fighting cybercrime including judicial authorities, LEAs, CERTs, and public and private stakeholders; with EC3 a central focal point for facilitating more effective operational coherence and a role for the European Police College (CEPOL) and Eurojust in providing the necessary training and information in order to allow stakeholders to effectively address cybercrime. The issue of collaboration and coordination between relevant actors has also been driven by the Digital Agenda for Europe, the Communication on Critical Information Infrastructure Protection (European Commission 2009) and the Progress Report on CIIP (European Commission 2011); the former in particular outlining that cooperation between CERTs and LEAs was essential (ENISA, 2012b, p.7), as did the EU's Internal Security Strategy (2010, p.2).[26]

This aspect also includes a strong international dimension which has several parts. The first is working with the Internet Corporation for Assigned Names and Numbers so that minimum (EU) standards are implemented in order to ensure that registered owners of websites can be identified by the registrar administering the name, in line with EU data protection rules. High standards of data protection are important 'as full compliance with data protection principles is an asset in effectively combating cybercrime', and importantly, it forms the basis of the required ecosystem to create a culture of sharing between member states – and passing on related intelligence to EC3 (Drewer and Ellerman 2012, p.2–3).The second relates to initiatives undertaken with international partners – a good example, as already mentioned above, being the Global Alliance against Child Sexual Abuse Online, launched in 2012 with 48 country members (54 at the time of writing – see Chapter 7) (EU–US Joint Statement 7–8 June 2012).

One of the most important aspects of coordination and collaboration in a cross-border context, is that of sharing data in real time (ENISA, A Flair for Sharing 2011), but for this to happen an ecosystem must be developed that removes legal (regulatory), technical and operational barriers and that allows trust to grow between different stakeholders – whether between public and private actors or those that argue over the right balance between rights and security in information exchange. Given the complexity and diversity that exists in working practices (culture), norms and indeed legal regulations on data sharing and collaboration, it is important that a level of harmonisation can be achieved that will allow efficient and effective policy on cybercrime to evolve.

Research that has been conducted thus far points to several problematic issues and challenges, as well as possible solutions to improving coordination and collaboration between stakeholders – that is, working in trust partnerships that allow the sharing of information and harmonised systems and processes at operational level, a key prerequisite for security as resilience to emerge. ENISA, in this sense, has been at the forefront of the studies conducted on the state of working practices between CERTs, and between LEAs and CERTs, and how such practices have evolved over the last five years (ENISA 2012a, 2012b). The central findings of the ENISA studies have pointed to several core issues that need to be addressed in order to ensure more effective collaboration and coordination. The first, related to the governance and operational level, is the issue of trust and integral to this, ways of working. This is important for CERT–CERT[27] and CERT–LEA cooperation.

In terms of CERT–CERT cooperation, it was found that 'in the main, cooperation and collaboration takes place in a practical, informal manner between operators who have trusted relationships rather than any strictly formalised legal agreement' (ENISA, A Flair for Sharing 2011, p.28). Thus a central tension that has existed in terms of cross-border CERT collaboration has been that of meeting legal obligations without undermining the effective informal channels of cooperation that exists between CERTs across Europe. Such informal trust relationships, it is suggested, are based on a number of factors, which are also important to understanding other public-private partnerships. These include: a) credibility, in particular in a technical sense (that is, whether the other party has sufficient knowledge and knows what they are talking about); b) Frequency of contact, in particular interaction through face-to-face meetings which fosters 'trust' relationships; and c) Identification and sharing of common intentions, where cybersecurity professionals are working towards the same objectives (Ibid., p.28).

In the case of CERT–LEA collaboration it was reported that the existence of informal mechanisms were critical in building effective and trustworthy partnerships, and that focusing on specific issues or problems such as botnets helped to galvanise cooperation (ENISA, 2012b, p.20). To this end, ENISA has played a critical role both in terms of bringing the CERT and LEA communities together to foster cooperation and indeed provide training and best practice guidance on various aspects of cybercrime – technical and policy related (see, for example, 8th ENISA workshop 'CERTs in Europe' 2013; ENISA, A Good Practice Guide for CERTs Directive on attacks against information systems 2013; ENISA Baseline Capability Policy Recommendation Report for national/government CERTs 2011; ENISA Work Programme 2012; Improving Information Security through Collaboration 2012). Trust has also been fostered in other ways – with examples of good practice including secondment of LEA staff to CERTs (for example, this is the case at CESICAT in Catalonia and the national CERT in Romania). However, trust can only be built and used effectively to combat cybercrime if the right regulatory and legal environment (governance) exists, in particular with regard to legislation on information and data exchange.

The importance of such informal and often ad hoc coming together of relevant networked stakeholders to tackle cybercrime – public and private – in trust relationships cannot be underestimated from a security as resilience governance perspective, as examples of actions to tackle botnets such as Conficker, Bredolab, Mariposa and others have shown (ENISA 2012b, p.22–25). However, lessons from Conficker also

demonstrated the need for some sort of sustainable and scalable collaborative framework, with a mix of informal and formal channels of communication for global incident responses, so that in the case of more complex and longer incidence response clarity, consistency and accuracy in information exchange could be maintained (Ibid., p.26).

The second issue relates to clarity – of role, function, definitions, procedures and capabilities of the actors involved; including training on how to understand and deal effectively with the procedural, legal and cultural aspects of investigating cybercrime. For CERTs, this is particularly salient as there are many different types – public and private – and CERTs in different countries have to contend with a variety of legal frames and grounds in order to determine what sort of information can be shared with other stakeholders in fighting cybercrime. In terms of CERT–LEA cooperation it was found that 'cultural' differences in terms of their focus and role presented significant challenges to collaboration between the two communities (see Table 5.2). Elaborating further, the ENISA study finds that, in line with its previous study (A Flair for Sharing 2011) the main legal challenges related to a discrepancy between the awareness of relevant national laws in comparison with international legal frameworks such as the Budapest Convention or the EU's Directives and Regulations. More specifically, awareness of national laws was much higher than relevant international laws – with a gap in particular in the knowledge on international law on data

Table 5.2 CERTs and LEAs: Culture and practice

	CERTs	**LEAs**
Focus on different definitions of cybercrime/attacks	Unintentional incidents; attacks against confidentiality, availability and integrity of IT	Where there is evidence or suspicion of a crime – which includes fraud or crimes where the confidentiality, availability and integrity of IT has not been affected
Character/working culture of each community	Informal, problem solving based	Procedural, rule based
Objectives of each community	Remediation	Prosecution
Direction of request	Inward (more likely to respond to requests)	Outward (more likely to transmit requests)

Source: ENISA (2012b, p.2).

privacy and protection – indeed, this was the second most provided reason for denial of provision of information, behind national security laws, of which, there was a high level of awareness, in particular among national/governmental CERTs.

This gap in knowledge between national and international legal rules creates a great deal of uncertainty with regards to information sharing and exchange – although potential solutions do not include further formalisation in the form of making information sharing mandatory, but rather developing 'frameworks for cooperation that were more error-tolerant, in which minor mistakes would not necessarily result in significant (legal) consequences thus permitting more opportunities for learning' (ENISA 2012b, p.51). Other challenges identified related to the scope and remit of CERTs and definitions of cybercrime – of computer and network misuse (ENISA 2012, p.2–3). Indeed an additional problem for CERTs – beyond the legal and regulatory obstacles to effective collaboration with LEAs – is the sheer number of stakeholders[28] that they are expected to interact with – all with differing expectations on the type of information that CERTs (national/governmental or private) can offer at any given point in time.

With regard to the operational dimension, a number of factors were identified that hindered information exchange and cooperation between LEAs and CERTs, primary among these in terms of process (denying a request) were: insufficient/inappropriate detail, issues of security clearance and wrong channel/addressee. The same reasons were given for receiving a denial of a request, with the addition of uncertainty (and omission of security clearance). In addition to this, issues relating to the role and parameters of cooperation were considered primary as a governance issue, followed by 'concerns over bureaucracy arising from different/unknown policies and procedures, lack of common standards, and lack of clarity on what the other party will do with information received' (Ibid.). An important observation from the research is that the importance of these factors varied according to the lifecycle of the institution (for example, the CERT) – where resource and understanding of legal frameworks might be less established at the inception stage than when it is more fully developed and experienced in navigating cross-border information exchange and the relevant legal frameworks for cybercrime incidents and investigations (Ibid.).

Particularly challenging within the legal and regulatory layer for information and data exchange are laws that relate to data protection and privacy which can be very stringent on how and when personal data can be used inside and outside the EU when connected to criminal activity

online. CERTs, for example, handle and process potential personal data such as IP addresses or user logs as well as, in certain circumstances if necessary for a specific type of incident, monitoring packet data (content of traffic). In doing this, CERTs need to ensure that they comply with the relevant national and European/international legal rules in order to 'avoid the possible suppression of any improperly gathered evidence that is intended to be presented in a court of law, as well as to avoid potential criminal or civil liability'[29] (ENISA, Flair for Sharing 2011, p.31). Clearly this process of sharing becomes even more complex once consideration is given to information exchange with a range of relevant stakeholders in the investigation and prosecution process – requiring expert knowledge of legal principles that most technically oriented, problem-solving CERTs do not have in-house. Establishing some sort of framework for data compliance and exchange would provide a more certain legal footing for effective information sharing through the life cycle of any investigation.

Clearly then, there are many regulatory (legal) and operational challenges in terms of collaboration and cooperation between the relevant agencies – intra- and inter-European but also global.[30] These raise important questions about creating an effective ecosystem within which a security as resilience can emerge for cybercrime – and point to further action that should be taken in the short, medium and long term in order to achieve this in relation to changing legal and procedural practices, operational tools and capacity, training, cultures of working, and governance mechanisms. In the long term, creating a more integrated working environment with the requisite expertise – legal, technical, operational – would certainly create procedural clarity and foster trust-based relationships through more regular interaction between key stakeholders in the fight against cybercrime.[31] As one senior Commission official put it, stakeholders 'need to see the added value of sharing information . . . and we need to push it to the operational level and create the right climate of trust' (Interview, DG Home, March 2013).

Some of these issues are addressed in the EU's cybersecurity strategy. For example, there is a focus on capability – at member state level – but also with regard to developing forensic tools through the support of the European Commission's Joint Research Centres (JRCs). To this end ten cybercrime centres of excellence have been established, funded by DG Home through the 'ISF Police' fund (formerly ISEC) – in Greece, France, Estonia, Czech Republic, Bulgaria, Belgium, Romania, UK, Spain, and Poland – that are engaged in the development of forensic tools, the creation of cybercrime training schemes and practical research into

issues affecting EU citizens (online fraud, telecoms fraud, cybersecurity of national critical infrastructure). In addition the European Academy of Law (ERA) was provided with EU funding for a project (2012–2015) to develop training programmes on legal and technical aspects of cybercrime (training for 500 judges and prosecutors). Other initiatives such as the European Cybercrime Training and Education Group (ECTEG) – have been tasked to build the capacity of European LEAs to combat cybercrime. Training packs have been completed and used to train over 1,500 cybercrime investigators in computer forensics and evidence collection, with a revised agreement (2013) signed between EC3, CEPOL and ECTEG to ensure updates to training curricula. Furthermore the EC3 (see below) has also delivered dedicated training, for example forensic expert training of skimming devices, investigating online child sexual abuse, as well as partnering with the ERA and ENISA to provide training on different aspects of cybercrime investigation. An issue that arises from these many initiatives is one of overlap, function and ultimately policy coherence[32] – the extent to which they join together with other EU agency work programmes, the uptake and adequacy of the training involved (and how this is compatible with domestic/local training) and the impact that this actually has in the medium to long run across the relevant stakeholders in the EU. According to one ENISA official, 'relationships [between the different bodies] are still formative' (Interview, ENISA official, August 2014) and need to be further developed to maximise synergies and avoid overlap.

Within the above context, the EUCSS highlights the importance of the operational role of Europol (EC3) in coordinating national member state investigations in cybercrime, primarily in the areas of child sexual abuse, payment fraud, botnets and intrusion. In addition, EC3 is tasked with ensuring that operational activities align with relevant EU policy, and with coordinating and collaborating with other relevant EU agencies such as Eurojust and CEPOL in order to ensure that the priority areas identified under the EMPACT policy cycle are addressed effectively. These include training, capacity-building, outreach, strategic analysis and technical support (see EC3 First Year Report 2014). This policy cycle was created by the Council of the EU in 2010 to essentially optimise cooperation between the relevant stakeholders – member states, EU institutions and agencies as well as third countries and organisations – in order to combat the primary criminal threats identified by the Europol Serious and Organised Crime and Threat Assessment (SOCTA). The SOCTA Report of 2013 (SOCTA Threat Assessment 2013) identified online payment card fraud, online sexual abuse and cyber-attacks on

information systems and critical infrastructure as the most important threats, with strategic goals and operational action plans then identified by the relevant EU actors and agencies to tackle them over the next four years.

In its first year of operation, EC3 faced both challenges and was also successful operationally through its different focal point teams[33] in assisting member states' law enforcement agencies to disrupt cybercrime networks. Indeed, overall it seems that in terms of other EU agencies 'the daily cooperation seems to be working well between them' (senior Commission official, DG Home, 2013). With CEPOL

> an alignment was made for structured cooperation; with the European Union's Judicial Cooperation Unit (Eurojust) working arrangements were agreed, including for the involvement of their liaison officer, and with the European Network and Information Security Agency (ENISA) the annual joint conference was organised, focussing on improving cooperation between computer emergency response teams (CERTs) and law enforcement.
>
> (EC3, First Year Report 2014, p.13)

The relationship between ENISA and EC3 has been one of mutual learning and collaboration – exchanging expertise on micro and macro aspects of cybercrime and cybersecurity, whilst also ensuring that there is a synergy and compatibility between the goals and objectives of each agency going forward (Telephone Interview, ENISA official, August 2014). To this end the heads of ENISA and Europol in June 2014 signed a strategic cooperation agreement to facilitate closer cooperation and exchange of expertise in the fight against cybercrime (ENISA Press Release 2014). Finally, new structures such as the Joint Cybercrime Action Taskforce (J-CAT) have been established – which includes EU and non-EU countries – to enhance operational cooperation capability in fighting cybercrime across Europe and globally. As noted in Chapter 4, this semi-formalised arrangement has already enjoyed operational success, but also highlighted some critical challenges if such arrangements are to work effectively going forward.

Whilst the EC3 operation to takedown the ZeroAccess botnet is a good example (see EC3, First Year Report 2014, p.13) of how cooperation can work in a successful cross-jurisdictional operation, it also raised certain challenges to the effective initiation and coordination of cybercrime with regard to the ability of EC3 to attain evidence and intelligence that was critical from private industry. A central issue has been that

of under-reporting of cybercrime to law enforcement – the fear from a business perspective, driven by an economic logic, that reporting major breaches could lead to brand damage and impact on profits. The result of this, however, for police forces and indeed prosecutors is lack of a comprehensive evidence base and picture of developments and trends in cybercrime activity, with the subsequent consequence that threats shared by others in private industry cannot be shared in real time to protect business. A related issue to information reporting by multinational companies (MNCs), in particular that of personal data is that of the process of reporting itself. Information received by Europol must be routed through the relevant member state unit responsible for cybercrime – but for many multinationals the information they have might not be related to the country in which they are based and thus generate a large number of reports that are not actually relevant to the national competent authority (NCA) of the country they are in. This then passes a workload and legal burden (responsibility and ownership of data) to the NCA which in practice is an obstacle to the effective flow of information from private industry to Europol and indeed LEAs in affected member states (EC3, First Year Report 2014, p.14).

This raises an interesting issue of governance modes and good practice – and in particular how to incentivise private industry to provide the information and which procedures can be utilised for reporting and getting relevant data to Europol. The proposed NIS Directive has made reporting mandatory for relevant sectors – but this will not resolve the problem faced by MNCs – or indeed address adequately the question of what exactly should be reported – which information and for which purpose (informal discussion on NIS Directive, Brussels, February 2014; Telephone Interview, senior official EC3, September 2014). Neither is it clear that mandatory reporting will incentivise private industry to participate in a more constructive way. Europol and ENISA, along with other industry and governmental voices have called for the involvement of the private sector in more systematic ways in order to meet the priorities set out for cybercrime and cybersecurity: with an example of good governance practice from the UK being that of swearing in specialists from the private sector on a voluntary basis, when required. Other examples include (albeit more structured) quarterly meetings between the Belgian cybercrime unit and Belgian card issuing banks, or Information Sharing and Analysis Centres (ISAC) for the financial sector in the US and Netherlands (House of Lords, EU committee, 13th Report of Session 2013–2014, p.15–17; Cybercrime @IPA, Special cybercrime units November 2011, p.38). Indeed, it is argued that such a hand-off

approach will create obvious incentives for industry to get involved in combating cybercrime and more effective and flexible partnerships, along with the processes and trust that are required to underpin them. Furthermore, such effective partnerships would allow for the ready use of expertise that exists in industry – in terms of systems, data and knowledge – which law enforcement agencies have a shortage of but see as essential (Interview, e-crime expert, July 2014).

A key prerequisite for effective security as resilience is the ability and preparedness to adopt new operating assumptions and institutional mechanisms. Given its mandate, EC3 has clearly done this very well within its first year, but despite this there are serious concerns about how far further effective progress can be made given the limited resources available to EC3 (a similar issue arises with ENISA as its mandate expands). Indeed the head of Europol, Rob Wainwright, has called for the next Justice and Home Affairs (JHA) programme of the EU to provide clear support to EC3 in order to fulfil its task more effectively going forward (House of Lords, EU committee, 13th Report of Session 2013–2014, p.15–17).

Even before its launch there was a great deal of uncertainty surrounding additional resource for Europol (EC3) to fulfil its mandate because of the financial crisis – with a decision that no additional staff or finance would be provided in its first year of operation (2013). It was only by moving money from existing internal budgets that EC3 was able to achieve some its major objectives – but this was to the detriment of not being able to develop mechanisms and tools for combating cybercrime that were originally planned. Whilst there was a budget increase of €1.7 million for Europol in the year 2014, with further budget increases for IT resource in 2015, the challenge will remain as to whether this resource will be enough to allow EC3 to fulfil its mandate effectively – in particular if increasing success brings with it ever more demands from different stakeholders. This concern is one that is stressed in the assessment of EC3 performance in its first year of operation where

> due to successes thus far, the current human and financial resources are already starting to constrain the progress of investigations. At the rate major investigations are coming in since the summer of 2013, EC3 will simply not be in a position to keep up. Increased resources, efficiencies, innovative approaches to cooperation, as well as capacity building among the broad range of partners, all need to be considered

> to maximise the impact on cybercrime and the criminals that benefit from it.
>
> (EC3, First Year Report 2014, p.32)

There is, then, a real question of ensuring not only sustainability of current operations and mechanisms, but also progress in terms of creating more innovative working methods, tools and processes in order that EC3 remains relevant and able to fulfil its mandate and address future challenges in cybercrime effectively (Interview, Senior Official EC3, September 2014).

The Commission's new proposal for a Regulation to enhance the role of Europol and create a European Union Agency for Law Enforcement (European Commission 2013) is an attempt to address challenges in information exchange and issues of resource and cost (for example through training, merging CEPOL into Europol and so on), as well as the legal and procedural issue of updating the law on Europol following the Lisbon Treaty (2009). This will have important implications for the work of EC3, even though it is likely to bring with it certain challenges in practice given that it will have resource implications and fundamentally change the relationship between Europol and member states.

First, there will be a step-change in terms of governance, with the Regulation introducing an increased obligation to provide data to Europol – with no exemptions, even if this conflicts with national security or the safety of individuals and integrity of ongoing domestic investigations relating to cybercrime. This is not likely to sit well with those member states that are already sceptical of EU involvement in what is still seen as an area of national sensitivity and interest. Second, there is also a step change in terms of the legal dimension – that is, hands-on meta-governance at the EU level. Whilst Europol can already request that a member state undertake an investigation the new Regulation includes an obligation for member states to justify and provide a reason if no operation is undertaken and any such reasons would be subject to challenge in the European Court of Justice. From one perspective this might be perceived as positive change towards accountability and effectiveness, but from a member state perspective it might also be interpreted as a risk to domestic operational independence and prioritisation, in particular in relation to cybercrime offences (UK Home Office July 2013). The proposed merging of CEPOL and Europol could potentially strengthen the synergies and links between training and operational requirements, thus helping to bridge a cultural divide between various

stakeholders, whilst also improving effectiveness of provision (Improvements proposed for Europol 2013), but evidence suggests that agreement will be difficult to reach on this with many member states opting to retain the status quo, despite there being a clear logic for merging training and operational dimensions into EC3 (Interview, Senior Official EC3, September 2014).

Conclusion: Security as resilience and European Union cybercrime

What does the above analysis point to in terms of an evolving security as resilience? What sort of implications does it have for the governance of cybercrime in the EU? It is quite clear from the above analysis that similar challenges exist now that did ten years ago with regard to constructing and optimising the preconditions for an effective security as resilience for combating cybercrime in the EU. The many actors, processes, levels, layers and dimensions involved in creating an effective ecosystem make this a complex exercise and one that can only be achieved through incremental change given the importance and centrality of transforming 'cultures' – ways of thinking and doing – in addressing the dynamic challenge of cybercrime. It is also clear that cybercrime – in reality – does not sit in isolation from the challenges of cybersecurity more broadly.

This is not to say that there has not been any progress – clearly there has in terms of creating mechanisms and spaces for developing a greater understanding of how different actors – such as, for example, LEAs and CERTs – think about and deal with cybercrime. Furthermore, many more member states within the European Union have now signed, ratified and implemented the Budapest Convention than had ten years ago – providing at least some basis for harmonisation and cooperation across borders that has been supplemented by the EU's Directives and Regulations that relate directly and indirectly to addressing cybercrime. It is also important to recognise that new institutional structures – prime examples being ENISA and EC3 – have been created to tackle the issue of cybercrime in terms of respectively, facilitating coordination among stakeholders within and between member states – and the operational aspects of cybercrime cooperation – from investigation to prosecution. At the EU level, also, the EUCSS (2013) has set out a list of priorities in relation to cybercrime as well as other aspects of cybersecurity – and there has clearly been a step-change in the legislation and governance of cybercrime that has sought to inject legal clarity into issues such as

the definition of a cybercrime, data and information sharing, privacy, and investigation and prosecution.

Developments have not just been in the legal, formal dimension. Networks, platforms, alliances and strategies have also evolved, such as the Safer Internet for Children and the European Strategy for a Better Internet for Children. The role of effective public-private partnerships has proven to be important – the European Financial Coalition, a good example here. It is also clear that evidence and opinion points to the salience of informal partnerships for the fight against cybercrime to work effectively. Such arrangements – in particular when issue driven (for example, the fight against botnets), clearly provide the flexibility and incentives for key stakeholders – public and private – to work together in order to optimise resource and expertise in combating cybercrime. Whilst the J-CAT initiative in this sense represents an attempt to (semi-)formalise such arrangement within EC3 structures, in the medium to long term it is still not clear how such a model can be scaled up to work systematically across Europe and globally in order to provide a more overarching and sustainable structure for public-private cooperation.

This said it is also obvious that the preconditions for effective security as resilience are far from being met within Europe and the EU – with the global and local dimensions adding further complexity to the evolution of a culture of cyber resilience. At the very basic level, the asymmetry between member states and the resources (whether that is financial, legal, skills and so on) they have for combating cybercrime presents a major hindrance with regard to preparedness, harmonisation, mutual recognition and convergence. Relationships between different stakeholders and agencies are formative and evolving – so whilst there is some convergence around the awareness of what is required – in practice there are still substantive barriers – cultural, behavioural, legal and political – to effective collaboration, coordination and cooperation. Moreover, whilst the EU has many initiatives to tackle cybercrime – what is still required is a sense of how they join together and indeed what sort of impact they are having with regard to operational, legal and regulatory, technical, training and cultural aspects across stakeholders. What we can safely conclude on the basis of the current evidence – and this chapter has by no means been able to cover all salient issues – is that security as resilience for cybercrime in the EU is formative but progressive – although not yet integrated to the degree that is required to combat cybercrime effectively across Europe and the EU. For this to emerge in the medium to long term barriers must continue to be

broken down between relevant stakeholder communities – and regular, sustainable working relationships and partnerships based on a common terminology constructed. Only in this way can the EU ensure that the ecosystem being developed to address the challenges of cybercrime and cybersecurity will allow Europe to protect its systems and networks against cyber criminals and ensure a secure platform for economic growth in the digital economy.

6
Network and Information Security and Cyber Defence in the European Union

Introduction

This chapter will address the remaining central strands of the Cybersecurity Strategy of the European Union (EUCSS 2013), namely those of Network and Information Security (NIS) and cyber defence. These two areas of cybersecurity policy are driven by two different mandates, and therefore very different processes and actors, even though collaborative structures on cybersecurity have now been established within the EU institutional milieu. Moreover, they are at different stages of development, with the issue of NIS part of the EU agenda for over ten years, and cyber defence only appearing more explicitly as a specific cybersecurity priority in the EUCSS. There will, thus, be a certain asymmetry in the balance of the analysis that follows, but it will nevertheless focus on the evolution of the two strands in the context of building resilience and indeed defence prior to the publication of the EUCSS and offer an early assessment of how measures outlined in the strategy might move the EU towards effective security as resilience in the near future. As with cybercrime, it must be emphasised here that these two strands whilst being analytically separated in this chapter, are very much interlinked – cyber defence is a critical element in securing systems and infrastructures against cyber-attacks. However, these two dimensions are 'governed' by very different mandates and therefore dynamics, which have varied implications for the evolving, even though overlapping ecosystem for both.

Several logics have underpinned the EU's approach to NIS. The first is an economic logic – to incentivise and stimulate the development of a secure information society for all. The second is a security logic, derived and very much linked to protecting critical infrastructure

against terrorist attacks. The EU's approach has also evolved in terms of governance logics, moving from a relatively hands-off approach to a more regulatory hands-on approach through the proposed Directive on Network and Information Security (2013) that was constructed alongside and very much as part of the EUCSS. Whilst the Framework Directive for Electronic Communications (2009a) imposed security and importantly, reporting obligations on electronic communications providers for telecoms providers and data controllers, the NIS Directive represented a clear step-change with regard to the governance rationale for *all* owners of critical infrastructure. That is, it proposed to extend the obligation to report significant cyber incidents to all relevant public and private actors in order to improve overall cyber resilience, including effective and coordinated collaboration and cooperation, in particular in relation to trusted information sharing (Proposal for an NIS Directive 2013a, p.3).

Beyond this, the European Network and Information Security Agency (ENISA) was established in 2004 in order to, in conjunction with the relevant stakeholders in the public and private sector, provide advice and recommendations on good practice in information security and facilitate collaboration and cooperation as well as implementation of relevant EU legislation on NIS. Indeed, the ENISA mandate was renewed in 2013, calling on the Agency to contribute directly to achieving cyber resilience and developing the industrial and technological resources for cybersecurity (Objectives 1 and 4 of the EUCSS).

In comparison to both cybercrime and NIS, cyber defence is a relatively new phenomenon – certainly in relation to the EU's institutional capacity and capability. However, EU action in this area has come from a growing realisation, certainly within the EEAS and its cybersecurity team, that 'cyber defence is an essential pillar of any cyber security strategy' (Interview, EEAS, senior official, Cyber Security team, February 2013). This has been underpinned primarily by a security logic that has emphasised the need to focus on detection, response and recovery[1] in order to increase the resilience of communications and information systems across the EU. Furthermore, given the multifaceted nature of cyber threats, the EUCSS has flagged 'the synergies between civilian and military approaches to protecting critical cyber assets' arguing that these need to be enhanced through various means, including research and development and further effective cooperation between relevant stakeholders (EUCSS 2013, p.11). In addition, cyber defence has been prioritised by EU member states through the EU's Capability Development Plan since 2011 and member states agreed on the EU Concept for

Cyber Defence in EU-led operations in 2012. Since then, the EDA and the EU military staff alongside the EEAS, European Commission and the EU member states have been involved as the main actors in developing cyber defence capabilities, which has also, inevitably, included an external dimension, with efforts in particular focused on NATO's existing policies and how the EU can complement these and avoid duplication.

This chapter will unfold in the following way in order to assess how far the EU has travelled in relation to NIS and cyber defence – assessing in particular the extent to which developments have moved the EU closer to – or further away from – achieving an effective security as resilience. The first section will provide a context for understanding EU policy developments in NIS and the logics and governance ideas that have underpinned them. Given that NIS has been intertwined with the EU's Critical Infrastructure Protection/Critical Information Infrastructure Protection policies and the Digital Agenda, it will provide a critical appraisal of action plans, Directives and proposals connected to these dimensions. The second section will then focus on the EUCSS and offer assessment of the proposals for improving cyber resilience. As comprehensive coverage of all elements is impossible within this chapter, it will focus on the role of ENISA and the proposal for an NIS Directive (2013), which at the time of writing (March 2015) is still under negotiation within the EU's Council of Ministers. The third section will then focus on cyber defence and in particular the objectives for cyber defence set out in the EUSCC and the proposals agreed at the European Council in December 2013 which set out five areas of work in relation to cyber defence. The final section will offer preliminary conclusions on how the EU has moved to effective security as resilience within these important strands of cybersecurity.

Governing NIS in the European Union

As was the case in the previous chapter on cybercrime, an economic logic has, in part, underpinned the EU approach to NIS as part of a broader information society programme. Thus the *e*Europe initiative (1999) and the EU's 'Communication on Network and Information Security: Proposal for a European Policy Approach', (European Commission 2001), highlighted the importance of information infrastructure protection, with the latter also providing recommendations on how to enhance security as resilience within the technical, legal and policy layer. The importance of the security of the Single European Information Space was also emphasised in the EU's i2010 initiative (2005),

which underlined the 'reliability and security of networks and information systems', as well as the European Commission's communication a 'Strategy for a Secure Information Society'[2] (European Commission 2006) that followed under the broader Digital Agenda for Europe initiative (European Commission 2010); the latter providing a comprehensive set of actions that were designed to address prevention, detection and response in relation to the challenges presented by network and information security.

The communication pointed to the need for the EU to establish certain important dimensions of resilience, including a culture of cybersecurity – with NIS and a regulatory framework for electronic communications making up two of the three pillars of any such strategy (the third being cybercrime, discussed in Chapter 5). The main initiatives within the communication aimed to enhance dialogue by encouraging benchmarking and the sharing of best practice among public administrations (open method rather than mandatory) in the expectation that this would also then raise awareness in the private sector. ENISA, in this sense, was encouraged to play an active role in this dialogue and in facilitating the exchange of best practices. A second initiative focused on information sharing through trusted strategic partnerships, with the aim of establishing a European information sharing and alert system to facilitate effective responses to threats to networks and information systems (European Commission Communication 2006a, p.8). Beyond this the communication also encouraged, among other things, technological diversity as an integral component of security, as well as openness, interoperability, and the ability for European industry to ensure the supply of secure network and information security products and services (Ibid., p.9).

The initiatives within these dimensions were designed to complement the objectives outlined in the Commission's Green Paper on the European Programme for Critical Infrastructure Protection (EPCIP) (European Commission Green Paper, EPCIP 2005) underpinned by a security logic and sectoral approach[3] – which for the ICT sector – meant enhancing the security and resilience of network and information systems through a multi-stakeholder dialogue approach. The ideas in the green paper were then further elaborated in the communication on a EPCIP (European Commission 2006b). This communication noted the interdependent and interconnected nature of critical infrastructures and the importance of ensuring the security of information technology as well as mitigating against other threats (terrorism, natural disasters, etc.), to their resilience. In this sense, the objective of the EPCIP was to

minimise vulnerabilities at the European level that might result from any breakdown in essential services and to improve and make more effective the protection and resilience of critical infrastructures in the EU. The central dimensions (the framework) of the programme emphasised the need for: a process to identify and designate 'European' critical infrastructures, and thus measures to protect them; procedural measures to help facilitate the implementation of the programme; the establishment of a Critical Infrastructure Warning Information Network (CIWIN) to exchange best practice in a secure way; increased support for member states concerning national critical infrastructure protection; and contingency and crisis management. There were also various measures outlined to ensure the implementation of the programme – including the establishment of a CIP Contact Group to facilitate coordination between member states, and also expert groups to build trust and facilitate coordination and information sharing between all stakeholders. In governance terms, the programme was reflective of hands-off metagovernance through the establishment of various information sharing and coordinative platforms.

What followed was a Directive that constituted a first step in identifying and designating European Critical Infrastructures (Council Directive 2008/114/EC).[4] This Directive focused on energy and transport and sought to set out more concrete procedures, mechanisms and platforms for identifying and designating European Critical Infrastructures (ECI)'s, and facilitating reporting, coordination and protection of ECI in these sectors.[5] The underlying rationale, of course, was to learn from this and how it might be applied to other sectors, highlighting ICT as a priority sector. No doubt also prompted by the attacks on Estonia in 2007, and building on the framework decision on attacks against information systems (and its planned revision), the Commission produced a communication on Critical Information Infrastructure Protection (European Commission 2009b), which highlighted some of the issues relating to achieving a security of resilience and proposed an action plan to address key challenges. These proposals sat in parallel to and under the EPCIP, and proposals to revise the EU's Regulatory Framework for Electronic Communications (discussed below). The issues touched on the failure to achieve basic essential criteria for security as resilience, including: the lack of coordination and cooperation across EU member states (dominance of national approaches and cultures) and uneven resource and knowledge (expertise) distribution; a problem of governance beyond national borders, with PPPs as the model of reference; differing processes and practices for monitoring and reporting network security incidents

and sharing information across member states (with basic requirements such as the existence of a National/Governmental CERT not in evidence across the EU); the lack of global cooperation and agreement on the governance and therefore protection of the Internet.

With regard to ensuring standardisation of reporting in relation to NIS breaches the revised Framework for Electronic Communications (European Parliament and Council 2009) aimed at adding a hands on meta-governance dimension – that is, it included legislation that made mandatory (Art. 13a) the reporting of any network and information systems security breaches to the national regulatory authority (NRA). This step-change was a significant move away from a voluntary approach (which characterised the 2006 communication, for example), with ENISA tasked in supporting member states to implement Article 13a through establishing a standard incident reporting methodology and mechanism (ENISA, Technical Guidelines on Incident Reporting 2013). The document produced by ENISA 'gives guidance to NRAs about the implementation of the two types of incident reporting mentioned in Article 13a: the annual summary reporting of significant incidents to ENISA and the EC and ad hoc notification of incidents to other NRAs in case of cross-border incidents'. It also defines the scope of incident reporting, the incident parameters and thresholds.

In the above context, the CIIP (European Commission 2009a, p.7–11) proposed five pillars of action: *Preparedness and Prevention* (to ensure preparedness at all levels) consisting of stakeholders establishing three essential aspects of cooperation and preparedness: 1. Defining, with the support of ENISA a minimal set of baseline capabilities and services that a National/Governmental CERT needs to have to function effectively; 2. European Public Private Partnership for Resilience (EP3R) to foster cooperation between the public and private sector with the aim of developing objectives for security and resilience, baseline requirements and good practice; and 3. European Forum for Member States (EFMS) to share good practice and share information on security and resilience of Critical Information Infrastructures (CIIs); *Detection and Response* to provide adequate early warning mechanisms which centred around the development, with ENISA, of an Early Information Sharing and Alert System; *Mitigation and Recovery* (to reinforce EU defence mechanisms for CII) involved a three-pronged but interrelated set of measures: 1. Developing national contingency plans and organising regular exercises for large scale network security incident response and recovery; 2. Developing pan-European exercises on Internet security incidents as a platform for participating in international exercises, for

example, US Cyber Storm; and 3. To reinforce cooperation between National/Governmental CERTs through already established fora such as the European Government CERTs Group (http://www.egc-group.org/); *International cooperation* (to promote EU priorities) mainly consisting of establishing European priorities on Internet resilience and stability and defining principles and guidelines for this at European and global levels; *Criteria for the ICT sector* (to support the Directive on the identification and designation of European critical infrastructures) which would aim to continue developing criteria for identifying ECI for the ICT sector through the commissioning of research on the topic.

There is a mixed picture with regard to how far these developments, in practice, contributed to constructing the necessary conditions for security as resilience to emerge. In the review of the CIIP (2011) conducted by the Commission, several achievements were noted related to each pillar, which would lead us to conclude, at surface level, that there was more than marginal success in what was recognised as an ongoing and dynamic exercise and concern.[6] This included: the establishment of National/Governmental CERTs in 20 EU member states,[7] with the ambition to establish a CERT for the EU institutions[8]; the establishment of EP3R and the EFMS; the development of a high-level roadmap for the implementation of European Information Sharing and Alert System (EISAS)[9]; 12 member states (at the end of 2010) establishing national contingency plans and the development by ENISA of a good practice guide on national exercises as well as the conduct of the first pan-European exercise, Cyber Europe 2010; the intensification of cooperation between National/Government CERTs; the establishment of European principles and guidelines for the Internet based on work undertaken in the EFMS; the participation of seven member states[10] in the US cyber exercise Cyber Storm III with ENISA and the Commission as observers; technical discussions on sector specific criteria for ICT in the EFMS leading to the development of draft criteria for fixed and mobile communications and the Internet.

However, evidence suggests that certain initiatives were more successful than others with regard to enhancing the conditions necessary for security as resilience to emerge, in particular in relation to establishing sustainable platforms for effective public-private interaction and collaboration. The EP3R, for example, was an exercise in learning but which ultimately did not produce any concrete outcomes in terms of creating a sustainable platform for public and private actors to discuss and construct solutions to real problems. Whilst the idea, born during the Tallinn conference of 2009, was positive, the initial two years of EP3R[11]

brought together public and private actors that did not have a clear focus on issues that needed to be discussed and resolved – or indeed, how any of the work being done in the various working groups set up would feed into broader EU policy on NIS. In the words of one observer, 'there was no real bind to the projects, the focus was not so clear, the terms of reference were quite broad and covering a lot of different topics' (Interview, Anonymous, July 2012). Ultimately, private actors were not provided with either the right incentives or indeed concrete issues and processes through which their expertise could be utilised in order to produce outcomes that would influence EU policy developments.

These shortcomings were recognised in an internal ENISA review of the initial processes that underpinned EP3R, which resulted in the emergence of clearer thematic areas for working groups and which included mission statements – ultimately, defining an agenda for work which was much more focused and goal oriented. The working group themes included: 1. Key assets, resources and functions for the continuous and secure provisioning of electronic communications across countries; 2. Baseline requirements for the security and resilience of electronic communications; and 3. Coordination and cooperation needs and mechanisms to prepare for and respond to large-scale disruptions affecting electronic communications (with a focus on fighting botnets). However, whilst this provided a greater focus to the work of EP3R in terms of objectives and potential outcomes, it did not 'get anywhere in terms of concrete deliverables'. Indeed, the EP3R platform suffered because it did not engender the conditions for trust to emerge among stakeholders – with different logics and views not allowing concrete outcomes to emerge (Interview, DG Connect official, June 2013, Interview ENISA official, July 2012). The fact that the work of EP3R was still not linked clearly to EU policy goals and legislation, did not provide the necessary incentives for private and public stakeholders to engage with any clear purpose.[12] The EP3R initiative was, following the publication of the EUCSS, subsumed under a new initiative, the NIS Public Private Platform (NISP) in order to address the shortcomings of the EP3R experiment. The NISP platform is explicitly tied to the EUCSS,[13] the NIS Directive and the H2020 programme of research[14] and at the time of writing (March 2015), it is still in the process of finalising its main deliverables, thus difficult to assess in terms of its utility and its sustainability as a platform. Suffice to say at this stage that some have already questioned how such an interim platform can be taken forward in the long-term to build the necessary trust and regular interaction needed for effective

public-private cooperation, coordination and collaboration (Interview, Anonymous, September 2014).

Beyond the EP3R, the EFMS, founded to enhance the coordination and cooperation between national governments on the security and resilience of critical infrastructure has not been as successful as some envisaged it might be. From one perspective, the UK government reply to the fourth report from the House of Lords EU Committee on CIIP Action Plan has clearly endorsed the platform, stating that EFMS 'has been a success and has tapped into a real need for policy makers to have an opportunity to exchange experience' (UK government House of Lords 2010–2011, p.8). Indeed it has played a key role in producing the EU's Principles and Guidelines for Internet Security and Resilience (see below). However, others have not been as complementary and have questioned the extent to which it has been able to facilitate real exchange of good practice or indeed information. For example, some have reported that it is a talking shop for junior officials with minimal concrete outcomes – and that it does not meet frequently enough, at only three times a year, to make any difference in terms of building trust and making more effective the sharing of information and good practice. Others have argued that such a platform is not seen as important as national-level platforms and coordination of national critical information infrastructure protection (Interviews, EEAS and ENISA, February 2013/July 2012; Interview, UK cybersecurity official, October 2014). More importantly, in terms of creating the conditions for collaboration, cooperation and coordination, the EFMS is seen as a useful tool, but not necessarily one that can create a sustainable, trustworthy and effective platform for discussion and exchange of information and good practice. In other words, whilst it provides the opportunity for policymakers to exchange experience and construct grand principles, beyond this, the outcome of this opportunity is not as obvious or transparent as could or indeed should be if issues of CIIP are to be addressed effectively and in a sustainable way within and throughout Europe.

In terms of European and global cyber exercises – these have been welcomed by national governments – and are perceived as positive instruments for enhancing the contingency planning and capability of EU member states in cybersecurity. The responsibility for cyber exercises was allocated to ENISA from the outset, which thus far has overseen two pan-European exercises (2010, 2012)[15] as well as joint exercises with the United States (see Chapter 7) and other third countries; it has also facilitated member states in their preparation and conduct of national exercises. The cyber exercises, at their inception, demonstrated

the asymmetry in the preparedness of EU member states in relation to attacks against information systems and critical infrastructure and the lack of any common European framework – rules, norms and ways of working – for responding and recovering from any such attacks. As one ENISA official involved in preparing the exercises noted in relation to the first exercise,

> there were expectations and capabilities . . . that was the biggest challenge . . . you had countries which were very much experienced and countries which are not as experienced . . . thus you have different expectations in terms of what they want from the exercises . . . and that is a major challenge . . . because not everybody is up to speed.
>
> (Interview, ENISA official, July 2012)

Having said this, it is also clear that the cyber exercises themselves have acted as a learning tool – that is, having to prepare for such exercises has also meant putting the necessary structures, institutions and environment (for example a CERT, contingency planning and so on) in place to be able to participate, and subsequently, respond in practice (Ibid.). ENISA, with the support of the Joint Research Centre of the European Commission (JRC) has facilitated the organisation and execution of exercises. To this end ENISA has published guidelines[16] and provided seminars for member states in order to provide clarity in what was involved throughout the lifecycle of the exercise. Thus cyber exercises were iterative learning platforms – where for each exercise challenges were encountered – but importantly, lessons were learnt on how to enhance both national level and European/global preparedness and response. What became obvious was that this was not just about technical improvement at different levels but enhancement of strategic, tactical, operational and political dimensions – of being able to react effectively in a resilient way to cyber-attacks. Thus in the evaluation of the first pan-European exercise in which only public entities participated[17] the challenges related to issues such as: the planning and structure of the cyber exercise; building trust; increasing understanding among the actors involved; points of contact in case of attack (single vs multiple points); and efficient communication and data exchange.

In terms of building trust, for example, the report noted that 'the fact that one representative (member state [MS] moderator) from each participating MS met and cooperated on a regular basis was probably the most significant trust building measure within the exercise' (ENISA, 2011a,

p.32). The important point here was that both in terms of increasing understanding and beginning to build trust, such a platform for information sharing and exchanging views was an essential starting point; indeed the frequency of meetings between those involved was critical not only for building trust but for increasing the understanding among member states of how to handle cyber incidents (Ibid., p.33). Overall then, whilst recommendations related to questions of pre-exercise preparation, format and structure (for example, on whether and how to include the private sector in future exercises), and importantly from a security as resilience perspective highlighted that 'the procedures on how to handle cyber incidents do not yet exist at a pan-European level' (ENISA, 2011a, p.9), as an exercise in building trust, understanding and information exchange it was recognised as a significant step from which improvements could be made. In the words of one ENISA official the exercise 'showed that it was really helpful for everybody, we really got to know each other in Europe' (Interview, ENISA official, July 2012).

The second cybersecurity exercise essentially took on board key lessons learnt from the first exercise, in particular in relation to including the private sector. This meant that including EU member states, European Free Trade Association (EFTA) countries (29 countries) and EU institutional participation, 339 organisations took part, with private and public actor cooperation essentially taking part at national level and public actor cooperation across borders (ENISA 2012c, p.4). The exercise was seen as a generally positive experience from all actors involved (88%), but it also revealed several key issues for the enhancement of security as resilience within and across Europe, as well as internationally. For example, at national level, whilst cooperation between public and private actors was generally seen as good during the exercise, it also became clear that cooperation was challenged due to different structures and procedures within countries. Issues also arose for public actors around the level of decision making at which crisis situations should be dealt with (for instance, which issues had to be escalated to strategic level). At the level of international cooperation, whilst again trust was built between the main participants involved, issues arose relating to improving knowledge of operational procedures in order to work with them more effectively, how to involve the private sector in a more systematic way going forward, the scalability and effectiveness of existing mechanisms and information flows for cooperation, and inclusion and input from other European critical sectors relevant to addressing any crisis situation (for example, transport) (Ibid., p.9–10). Overall, this exercise was instructive – with again perhaps the most valuable lesson

learnt that as a platform for enhancing learning on the technical, political (institutional), operational and strategic levels, it was effective, and should continue to be utilised as a key tool for enhancing knowledge, understanding and trust among key stakeholders.

Finally, in terms of the objective for defining principles and guidelines for Internet resilience and stability, the EU published a document in March 2011, which was a result of discussion and deliberation in the EFMS. To this end the outcome reflects both the positive and negative aspects of such as forum; that is, such a forum has a valuable function with regard to producing general statements of principle on cybersecurity and resilience, but perhaps less so with regard to micro elements of effective cooperation and collaboration across the relevant stakeholders or specific issues such as intelligence and information sharing. On the positive side the document defines a clear set of guidelines and principles which underscores the normative underpinning of EU policy on Internet resilience and stability – if not operational, strategic and tactical ways of achieving it (which is subsequently addressed in the EUCSS). It offers clear a political statement on what the Internet should and should not be and the requisite governance to secure it. Thus the EU conceives of the global Internet as a public or collective good that should be available to and accessible by all. That is, there is a normative view that use of the Internet should not be restricted or limited to any citizen, the exception being with regard to measures and instruments that are used in order to prevent harm to others. Furthermore, when it comes to cybersecurity, it is clear that EU core values, laws and norms are as central to online activity as they are offline and that 'Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union . . . ' (EUCSS 2013, p.4).

Beyond this, there is also a very clear EU idea on the governance model of choice for the Internet and cybersecurity policy more specifically, that of multi-stakeholderism (see European Commission 2009b; and EUCSS). This model, of course, is not without controversy. Whilst the multi-stakeholder vision is born from the very complexity of the Internet in terms of the many actors involved in its management and use – and is shared by many 'Western' states (for example, US, Japan, Canada, and Australia), it is highly contested by those states (for example, Iran, Russia, China and India) that consider (a) the US to hold too much power over the management of the Internet (b) themselves to be under-represented in the existing global Internet

governance institutions and that wish to see much more governmental involvement in cyberspace through the ITU – that is, a traditional hands-on intergovernmental rather than a multi-stakeholder approach (see Chapter 3).

The importance of the involvement of all stakeholders is also reflected in the EU's principle of shared responsibility for the effective security of cyberspace. In this sense, this runs throughout the additional principles and guidelines that the EU presents as critical for Internet resilience and stability, including that of improving education and raising awareness, internal EU cooperation and mutual assistance, creating a strong ICT industry in Europe (ensuring diversity of products), good risk-management and the construction and uptake of open standards with security and privacy built in from the design phase (European Principles and Guidelines 2011). Also significant is the emphasis that the EU places on the global context and international cooperation. The EU is all too aware that any EU principles on cybersecurity do not exist in a vacuum, and that, without cooperation and collaboration with international public and private partners to create global principles compatible with EU values, the EU's attempts to construct its own resilient cybersecurity policy will be fundamentally weakened, as will the stability and interoperability of the Internet.

Global disagreement and contestation, for example, on the role of technical standards, data protection and privacy, who should control and regulate the Internet, and the appropriate legal conventions and protocols for fighting cybercrime and cyber-attacks can undermine any attempt to create a secure and resilient cyberspace for all. Whilst the EU primarily supports a multi-stakeholder approach for the governance of the cyber world, it is also clear that public authorities have an important role to play in providing a normative and legal framework for the activities of all stakeholders. In other words, the EU supports within the multi-stakeholder umbrella a specific type of public-private partnership, where public authorities should decide (in consultation with relevant stakeholders) on the appropriate modes and forms of governance and regulation (for instance, incentives) and where the private sector has an important day-to-day role in the management of the Internet and its security (European principles and guidelines 2011; EUCSS 2013, 3). In this sense, the EU, in particular in the post-Snowden era, has also supported a greater role for the Governmental Advisory Committee in ICANN, to give it a greater decision-making role in policy on Internet governance.[18]

Network and information security in the cybersecurity strategy of the European Union: Achieving cyber resilience?

The above view of achieving resilience is very much reflected in the proposal for an NIS Directive that accompanied the EUCSS. Indeed, the Directive acknowledges that it is a step-change (European Commission 2013a, 4) from hands-off meta-governance to a more hands-on mandatory stance towards improving capability and reporting of major cyber incidents and managing risk. The Directive obliges not only the telecommunications providers and data controllers sector as was previously the case under the Framework Directive for Electronic Communications (2009), but all sectors which are deemed to be owners of critical infrastructure (energy, banking, transport, stock exchanges, public administrations). As noted in the EUCSS (2013), although some progress had been made under a more voluntary arrangement with regard to cultivating a culture of cybersecurity, 'gaps remained across the EU' and private actors lacked 'effective incentives to provide reliable data on the existence or impact of NIS incidents, to embrace a risk management culture or to invest in security solutions' (EUCSS 2013, 5). The proposal for the NIS Directive (European Commission 2013a, 3) is even more explicit in acknowledging that, 'The current situation in the EU, reflecting the purely voluntary approach followed so far, does not provide sufficient protection against NIS incidents and risks across the EU'.

The NIS Directive and the regulatory (governance) approach taken within it was constructed as the most optimal option[19] for incentivising governments and business to adopt practices that would lead to a more effective security of resilience, through: obliging member states to ensure adequate institutional preparedness, such as competent authorities for NIS and a functioning national/governmental CERT; establishing prevention, detection, mitigation and response mechanisms to enable information sharing and mutual assistance among national NIS competent authorities, and for the latter to also ensure EU wide cooperation on the basis of an EU NIS Action Plan designed to respond to NIS incidents with a cross-border dimension; and improving the engagement and preparedness of the private sector through obliging them to report major NIS incidents to national NIS competent authorities (European Commission 2013a; EUCSS 2013). The overall logic of the Directive is underpinned by the assumption that 'obligation' – to prepare and develop capabilities on the part of member states and to report incidents on the part of private actors and relevant public administrations –

will better contribute to establishing a climate of mutual trust and thus more effective cooperation and collaboration within and between the public and private sector. That is, it will better facilitate and nurture the emergence of the conditions necessary for effective security as resilience. At the same time, the Commission recognises and encourages the continued use and utility of informal and trusted channels of information sharing between relevant stakeholders in order to improve security and exchange information and good practice.

It is perhaps not surprising that the NIS Directive has received general support with regard to the principle of protecting NIS against threats but that it has also received a great deal of criticism with regard to the detail of how this should be done. This criticism has not simply come from private industry but also governments and other EU institutions, in particular the European Parliament, and has led to significant revision and one could argue deliberate watering down of the Directive. For example, the purpose of the original Directive was to include all sectors and actors that were relevant to the protection of critical infrastructure: however, some member states have argued that the NIS Directive – derived from an internal market mandate – was not the appropriate legal base for including public administrations given that it touched upon issues that were potentially 'security sensitive'. Germany in particular insisted on and achieved the removal of public administrations from the list of actors that would be included within the remit of the NIS Directive. Similarly, the Internal Market and Consumer Protection (IMCO) committee of the European Parliament, in the words of one of its members, 'pursued a strategy of making it vague' (Informal meeting, Brussels, February 2013) following concerns about scope, and a lack of detail on how it could be implemented. More specifically, IMCO reduced the scope of the Directive further by removing the inclusion of so-called 'Internet Enablers'[20] – arguing that this was unnecessary, not fully justified (for example, why include Internet enablers and not hardware/software manufactures?) and challenging – and that in governance terms, voluntary trust relationships would be more beneficial than a mandatory approach.

Aside from these specific aspects there is also still some debate among and between industry and governments with regard to the governance model being pursued to achieve cyber resilience. There are several dimensions to this. First, there is the issue of cost which stems from an applied economic logic in the relevant sectors affected. This not only relates to the financial implications of administering a mandatory reporting system but also issues such as the threshold for reporting,

information on the powers of the national competent authority, and other unintended consequences including, importantly, incentivising movement to a tick-box compliance and audit culture rather than a stronger and more effective cybersecurity culture. As noted in the Report on Responses to the NIS Directive in the UK, 'Stakeholders flagged that mandatory reporting would create a compliance culture; this would stifle voluntary information sharing and resources that would be allocated to developing cybersecurity capability [which] would be reallocated to employing legal teams to analyse each incident' (UK Department of Business Innovation and Skills Report September 2013, p.23). Second, and interrelated, there is a fear that the NIS Directive could impact negatively on the culture of dialogue between the public and private sector – the movement away from dialogue and collaboration to top-down obligation to report, it is argued by some, could divert resources away from effective security measures and undermine the benefits that companies gain from voluntary bi-directional (informal) exchange which improves understanding of new threats and improves incident response. There is also the argument that if this obligation to report is too burdensome it could weaken trust at a time when real-time information sharing and collective responses are critical. This is even more important in the post-Snowden era where confidence and trust are low in terms of information sharing from the private to the public sphere.

The above argument is important as the NIS Directive rests on the key assumption that a mandatory hands-on approach will bring about the most effective security as resilience by incentivising through obligation and sanctions. This assumption, which the Commission has argued was supported by a significant proportion of those consulted on the utility of making capability and reporting mandatory (see European Commission 2013b) has been questioned, however, not least because only a small proportion of those that responded (approximately 15%) were actually from the sectors affected by the Directive (UK Department of Business Innovation and Skills Report, September 2013, p.14). So, whilst a majority of respondents did support strengthening NIS capabilities across Europe, and measures such as establishing CERTs and competent NIS authorities, that is – general minimal harmonisation – it seems that among those sectors directly affected there is little consensus on whether mandatory reporting would make for a more effective security as resilience. Thus, evidence is inconclusive on the matter, although there is a strong argument from certain parts of industry and practice in certain EU member states that a voluntary, sector specific approach is much more dynamic, and underpinned by an informal, trust-based

relationship. In this sense the counterargument or narrative to that in the Directive is that of essentially making more systematic such an arrangement through a mixed approach (regulatory and voluntary) in order to improve capabilities and reporting across Europe (Interview, UK official, October 2014).

Finally, there are also certain broader issues that could affect how far the Directive contributes to improved security as resilience within Europe. The first of these relates to CERTs. There are already over 100 CERTs around Europe – public and private – and the NIS Directive will mandate the requirement for a well-functioning national or governmental CERT in each member state of the EU – to improve capability, cooperation and collaboration. There is also a proposal to examine the feasibility of setting up CERTs for industrial control systems. However, despite such progress, it is not clear how the NIS Directive will contribute to actually addressing the quality of the CERTs established – and in particular how it will incentivise CERTs to be more proactive rather than reactive. As ENISA has noted, 'The most common approach used by CERTs to handle security incidents is to wait for incoming incident reports, then try to "treat" the effects of the attacks but not necessarily treat the "cause". In this case the incident already happened and potentially had an impact on the production environment' (ENISA 2011b).

There are also additional problems related to the reactive nature of CERTs that need to be addressed in order to allow CERTs to become more operationally effective. They range from CERTs not utilising all information available to them from external sources, not collecting incident data from other constituencies, and the poor quality of data collected, to legal issues such as regulations on privacy and data protection which can hinder the exchange of relevant information. This is certainly an issue that has also been raised with regard to the objectives of the NIS Directive in a post-Snowden era, in particular the potential conflict with the revised EU Data Protection Regulation. Obviously information exchange is critical as part of one of the conditions for achieving effective security as resilience – not just with regard to CERTs – but across the different spectrums, layers and actors involved in cyber resilience. It is not clear how far – through the EUCSS and the NIS Directive – the EU and ENISA will be able to incentivise CERTs to make the necessary changes and build capacity in order to become more effective.

Second, the NIS Directive offers little clarity on issues such as reporting within the more complex ecosystem of cloud computing. In effect the Directive will place responsibility on competent national authorities

and relevant private and public actors for reporting breaches in their control even if they are outside the EU, which might get complicated if the service being used by them is located in, for example, a country which does not adhere to EU standards – in this case the relevant competent national authority or public and/or private actors risk failing to comply with the Directive because there is no requirement to essentially sign a contractual framework agreement between the EU body and service provider in other countries. This problem is also exacerbated by the fact that not all countries have signed up to a global framework for dealing with cybercrime (including cyber-attacks on information systems), such as the Budapest Convention. Third there is also an issue of creating a common reporting standard – and related to this the need for a coordinated implementation of the Directive to avoid fragmentation. ENISA, here, has a key role to play to facilitate effective implementation and also ensure the establishment and functioning of a common reporting system as it has done with Article 13a of the Telecoms Directive and Article 4 of the e-privacy Directive. Despite this, concerns remain about the specifics of information sharing required by the Directive – in particular in relation to what has to be shared, how the information will be used, and the impact this might have on existing information sharing and intelligence gathering activity (Informal meeting, Brussels, February 2013).

Finally, there is the issue of how much the governance approach taken in the NIS Directive diverges from the US approach, which is voluntary in nature, despite attempts to approve administration-backed cybersecurity legislation in November 2012, which met with fierce opposition from business groups complaining of over-regulation. The main implication here is that despite collaboration through the EU–US working group on cybercrime and cybersecurity and the EU–US cyber dialogue (see Chapter 7) there will clearly be different rules at work in Europe and the US with regard to reporting obligations. This, in turn, will threaten inconsistency for those companies that span both jurisdictions – as well as having implications and consequences in terms of trust and cooperation. This could also pose a major obstacle to the negotiation of any free trade deal between the US and Europe in the near future.

European Union cyber defence: Under construction?

In the EU's review of the EUCSS after its first year the cyber defence dimension was assessed, in most part, as 'under construction'. The idea

of including a cyber defence dimension in the EUCSS was to enable the EU to develop a 'comprehensive' or 'whole-of-union' approach to cybersecurity, in the knowledge that this was the least developed priority area, but one that was essential to an effective security as resilience in Europe. It became clear that critical military functions, processes and actions were dependent on the cyber domain, and more specifically, on civilian critical infrastructures and processes. This alongside the constant and rapid growth of complex and interconnected networks meant new vulnerabilities and threats emerged that had to be addressed for the military to operate securely and effectively in its day-to-day work. To this end, cyber defence was a top ten priority area in the EDA Capability Development Plan (CDP) in 2011, which set a number of tasks for realisation in this area, including the production of a cyber defence landscaping study, the development of a cyber defence training curriculum, assessing the feasibility of the establishment of a European Cyber Defence Centre (ECDC) and keeping track of relevant research and training activities (Cirlig 2014; Roehrig 2014). EU member states agreed on the EU Concept for Cyber Defence in EU-led operations in 2012 allowing operational commanders to create and maintain situational cyber awareness. In turn, the European Council of December 2013 (European Council Conclusions December 2013), in its discussions of cyber defence, reiterated the need for work to continue and evolve in five key areas:

1. To promote the development of EU cyber defence capabilities, research and technologies through an EDA cyber defence roadmap
2. To develop a cyber defence policy framework to protect networks supporting CSDP institutions, missions and operations
3. To improve cyber training, education and exercise opportunities for member states
4. To strengthen cooperation with NATO and other international organisations, the private sector and academia
5. To develop early warning and response mechanisms and to seek synergies between relevant cybersecurity actors in Europe

At the same meeting, Catherine Ashton, the EU's High Representative at the time, was tasked, in cooperation with the European Commission and the EDA, to develop an EU cyber defence policy framework within which the above actions could be delivered. The role of EDA was particularly important in this, concentrating on training, improving cyber situational awareness, improving civil and military cooperation,

the protection of EU assets during missions, and operations and technological aspects.

It is important to realise that when talking about cyber defence in the EU, this does not mean the development of offensive cyber capability (as is the case with the US, for example) but rather 'cyber self-protection and assured access to cyberspace to enable conventional military activity' (Roehrig and Smeaton 2013, 24). A key starting point for realising the actions for cyber defence was to establish, in the first instance, a deeper understanding of capabilities across Europe. In order to achieve this, the EDA commissioned a study that included the 20 EU (EDA) participating member states,[21] and which analysed cyber defence capabilities at national level as well as EU-level organisations involved in cyber defence activities in the context of CSDP missions[22] (Cyber Defence Fact Sheet 2013). The findings, from a security as resilience perspective, suggest that whilst key conditions are certainly being met, many challenges remain. For example, at the level of the EU, it is suggested that threat analysis and intelligence gathering capability is emergent and incident response needed to be deepened within the complex organisational set-up at operational level – that is, between the EDA, EEAS, General Secretariat of the Council (GSC), the Council of Ministers, European Commission, ENISA, EC3 and the EU-CERT. In addition, it reveals that knowledge and understanding of military specific standards and tools is poor and that the culture of good cybersecurity practice needs to be nurtured in order to make it more effective (Cyber Defence Fact Sheet 2013).

At the EU member state level, the picture is reflective of cybersecurity preparedness more generally. That is, although progress has been made across Europe in the 20 member states assessed, much variability in capability still exists and thus there is much room for improvement. Capability in this study was evaluated across six key domains[23] which included: leadership, personnel, interoperability, doctrine, organisation, training and facilities. In general, the results show that member states with a high level of maturity in their thinking among key decision makers about cybersecurity are also more advanced in relation to cyber defence capability. More specifically, the study also revealed that the strengths across the 20 member states were found in the areas of leadership, personnel, and interoperability, and that with regard to key military decision makers no country reported a poor level of familiarity with cyber defence issues. However, with regard to doctrine, organisation and training, lower levels of understanding and maturity were found; this difference potentially linked to the fact that in the latter more complex, longer-term, organisational structures and processes are

required. Within the facilities domain the situation was reported to be even less developed and virtually non-existent in many instances (Cyber Defence Fact Sheet 2013; Robinson et al. 2013).

To elaborate further on this, it is clear that the EU participating countries in this study have struggled with the doctrinal aspects of the role of the military in defending cyberspace. There has been confusion or at least little clarity on the function of the military in the cyber defence domain and the relationship between broader national cybersecurity strategies and cyber defence doctrines developed by the military. This aside though, certain EU countries that are considered as advanced in their cybersecurity thinking – France, the Netherlands and the UK – have created military based CERTs (milCERTs) and are at different stages of evaluation and implementation with regard to more organic cyber defence organisations (Robinson 2014, p.2). On developing cyber defence doctrine EU countries and indeed the EU are not considered to be at an advanced stage, and are encouraged to improve this in close coordination with other EU member states and EU institutions.

In terms of cyber defence training and education, much is also still to be done with a particular deficit identified in provision at operational and senior command levels. Issues at the EU level exist with regard to creating a culture of cybersecurity one solution to which includes, potentially the establishment of a pan-European Task Force to establish good practice, raise awareness and provide training in cyber defence issues. Indeed identifying synergies and developing further a cooperation model with EU actors that are engaged in the provision of training – such as EC3, ECTEG, ENISA and the European Security and Defence College (ESDC) – would enhance both training and intelligence capability. In order to facilitate the development of training for cyber defence the EDA undertook a cyber defence Training Needs Analysis (TNA), which has built on existing training courses in the EU and its member states and which has been done in close cooperation with the CCDCoE in Tallinn.

The central objectives of this TNA included providing a more clearly defined and targeted training regime that delineated different levels (defined target audiences), types of cyber defence training (appropriate for each level) and functional requirements (support and training tools). Indeed, actions have already been developed in this field,[24] prominent among these the EDA ad hoc project on cyber ranges (to test cyber defensive capabilities) which aims to: increase the availability of cyber ranges; increase the efficiency of existing cyber ranges; establish a cyber ranges network; and to improve cyber defence training exercises and

testing at European level in the medium term (Roehrig 2013). Within and throughout the EU then there are existing opportunities that need to be leveraged further, in particular in relation to joint exercises – bilateral and collective (ENISA, NATO) – and training, as well as new training and education structures that need to be established. It is also obvious though that the asymmetry within Europe necessitates further action if more effective security as resilience is to result within the cyber defence ecosystem. That EU Defence Ministers in 2012 agreed to put cyber defence on the Pooling and Sharing agenda will facilitate further joint working on training and education, and allow the EDA to explore further synergies that will contribute to enhancing capacity in this area, including, importantly, growing and retaining high quality cyber specialists in the military.

As certain commentators have pointed out, reinforcing the protection of communications and information networks for CSDP institutions, missions and operations, raises complex issues, not least because the EU does not actually possess its own organic military assets (Roehrig and Smeaton 2013, p.24; Robinson 2014, p.2). Moreover, it raises questions of how to reconcile individual member state responsibilities for critical infrastructure in home contexts and of how to engage with the private owners of relevant critical infrastructure (Robinson 2014, p.3). Thus, that EU military operations have a high dependence on essentially privately owned critical infrastructure and civilian actors, raises issues of cooperation and synergies between the two and how to achieve this most effectively. More specifically, it raises questions related to cultural approaches to managing risk and protection, including in relation to assurance and indeed security standards. The EU is not devoid of organisational capacity for addressing these issues – for example, the EU military staff (EUMS) and the Council of Ministers are continually upgrading communication and information security capabilities, and the CERT-EU has advanced in terms of its own maturity levels and ability.

However, there are also potential issues with embedding cybersecurity into crisis management related to complex CSDP planning processes and more specifically, the different phases of missions, that is, the strategic appraisal phase and the force generation phase. Here, any Operational Commander would have to be clear on how to assess and understand potential cybersecurity exploitation points for any given mission (strategic appraisal[25]) and how to strike a balance between assets mobilised in the operational context and the cyber defence capabilities of member states offering assets for any particular mission (force generation). In developing the proposed cyber defence policy framework then, clarity would be needed for how cyber risks are decided, assessed

and operationalised in any mission if cyber defence is to be effectively mainstreamed into CSDP structures (Ibid.). Finally, these points are very much interlinked to enhancing civil-military cooperation not just in operational practice but in training – in order to create a better understanding of the shared risks and practices required to address them in cyber defence (for example, participation of milCERTs in national and multinational civil crisis management exercises or govCERTs in national and multinational military exercises).

The final area of action – strengthening cooperation with NATO and other relevant international, public and private actors – is one in which the EU is making some progress but where effective partnerships could certainly be enhanced. EU–NATO cooperation at the informal level has been ongoing since 2010, and has yielded agreement on common areas of concern such as raising cybersecurity awareness, and training and capability development in terms of cyber resilience. Whilst NATO itself has been undergoing its own identity transformation in the last few years, it has enhanced its policy and established an action plan through which to develop cyber defence capability – to address both the civil and military dimension. The enhanced policy was endorsed at NATO's Wales Summit in September 2014, with the top priority 'the protection of the communications systems owned and operated by the Alliance' (NATO 2014).

Beyond this though, it also emphasised facilitating the efforts of NATO allies in cyber defence (22 EU member states are of course also members of NATO), the enhancement of its own institutional capability and capacity, and cooperation with partners and industry. Institutionally, NATO has established Rapid Reaction Teams for Cyber Defence, a Computer Incident Response Capability to protect its own networks which works with its Cyber Defence Management Authority, a Defence Planning Process which 'defines targets for Allied countries' implementation of national cyber defence capabilities', and cyber defence has also been integrated into its Smart Defence Initiative which enables countries to work together to develop cyber defence capabilities where they otherwise could not do so alone[26] (Ibid.). Beyond NATO formal structures for cyber defence, the NATO-accredited CCDCoE in Tallinn is an active authority in the field of cyber defence education and training, as well as research and development. Indeed, it published a landmark document – the Tallinn Manual (see also Chapters 3 and 7) – on the interpretation of the Law of Armed Conflict as it relates to cyber defence.

The task for the EU then in its quest to construct a policy framework for cyber defence, and indeed a more effective security as resilience

in this field, is to examine how cooperation and partnership can be established which avoids duplication and makes full use of sharing and pooling resources where possible. Whilst formally there are many obstacles to this, processes and agreements similar to those that have been constructed for shared 'defence' resource and capability, are a possibility and an avenue that could be pursued for cooperation between the two. Beyond NATO, the EU's most advanced international partnership is with the US through the EU–US Working Group on Cyber Security and Cybercrime, but this does not have an explicit cyber defence dimension (see Chapter 7). Similarly the EU has signed agreements and has a cyber dialogue platform with India, Brazil and China (for example, an EU China Cyber Security Task Force has been created), and has participated in various high-level diplomatic conferences (for example, in London 2011, Budapest 2012, and Seoul 2013), organised to deliberate on norms and rules for the governance of global cyberspace. The latter formal platforms, however, whilst effective for reinforcing key messages in relation to preferred norms for the Internet, have not resulted in any effective partnerships in relation to cyber defence, and are rather too infrequent to yield any practical agreement on shared practice or common understandings of cyber defence challenges.

Conclusions

This chapter has offered an assessment of two of the EU's priority strands in its cybersecurity strategy. As indicated in the Introduction to the book – the coverage – in particular related to NIS – could not be comprehensive given the broad scope of the topic – indeed critical issues such as security of the cloud, mobile networks, smart grids, IT-enabled industrial control systems, cooperation on the standardisation process and so on, have been omitted. This aside, there are important general and more specific implications that arise for the EU's security as resilience in relation to NIS and cyber defence.

In terms of NIS there are differentiated patterns across member states with regard to capability and cooperation – and it seems a lack of willingness under a voluntary regime to report incidents and enhance institutional capacities for cyber resilience. The European Commission argued that there was a lack of incentive for the public or private sector to enhance capabilities which led to the proposed NIS Directive; the centrepiece legislation that accompanied the EUCSS – which signified a clear step-change in the governance of NIS – to a hands-on meta-governance approach. On the main objectives of the proposed

NIS Directive – to enhance cyber resilience, there has been a general consensus – but also many perceived issues and challenges that might limit it establishing the critical conditions for effective security as resilience in terms of promoting cooperation, collaboration and coordination and a culture of cybersecurity in terms of trust based partnerships required for information exchange and information sharing between relevant stakeholders. On capability, there is a general consensus that establishing minimal institutional capacity would be positive, although ensuring the quality of the institutions and their practice might be much more difficult to achieve. NIS is certainly progressive in creating the necessary conditions for cybersecurity as resilience – with examples of good practice abound – but far from optimal.

This said, for cyber defence the conditions for security as resilience are formative at best. Such a conclusion is not surprising given the relative newness of the area on the EU's cyber agenda, but developments are accelerating at pace, with the EDA leading on important priority areas. A clearer idea of the landscape has emerged with regard to cyber defence capability at EU level and within EDA participating member states, but so too the challenges ahead in this area for the EU to achieve its main objectives and develop an effective and comprehensive framework for cyber defence. Clearly, awareness, understanding, institutional and organisational capacity are in their infancy at EU level – with a mixed picture at member state level that makes for incoherence and ineffectiveness in cyber defence.

Platforms are being established – and progress is slow but emerging in terms of moving towards a more effective and resilient regime. Strands such as training and education are more highly evolved than others at European level, with ad hoc projects operationalised by the EDA to enhance knowledge and capability. At member state level, however, issues remain for many with regard to constructing the necessary facilities, organisations and doctrines for the development of cyber defence. Whilst potential exists for the evolution of more effective international partnerships to address cyber defence issues, here too, progress is constrained by complexity in the formal process – in particular in relation to NATO – even though obvious synergies exist. Moreover, not all member states of the EU participate in the cyber defence pillar – underpinned by a CSDP mandate – making it more difficult for shared understandings and approaches to emerge at EU level in the near future.

7

Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience?

Introduction

Cybersecurity is a global challenge (see Chapter 3) that requires international collaboration and partnership with key actors and organisations if it is to be addressed effectively. In this context, a European Union (EU) priority within its cybersecurity strategy is to establish a coherent international cyberspace policy and to promote and project EU core values for cyberspace. The EU's cybersecurity strategy (EUCSS) states that its international cyberspace policy 'will be aimed at increased engagement and stronger relations with key international partners and organisations, as well as with civil society and the private sector' and that at 'bilateral level, cooperation with the United States is particularly important and will be further developed', notably in the context of the EU–US Working Group on Cyber-Security and Cyber-Crime (European Commission 2011; EU Cybersecurity Strategy 2013, p.15). Indeed the Working Group was established to 'tackle new threats to the global networks upon which the security and the prosperity of our free society increasingly depend' (Joint Statement of the EU–US Summit 2010).

The relationship with the United States (US), it can be argued, is valuable to Europe not just in terms of cybersecurity and cybercrime *per se* but critically, and more broadly, in terms of transatlantic trade flows and the negotiations on the Transatlantic Trade and Investment Partnership (TTIP). These issues are inexorably linked through mechanisms for sharing real time digital data and information – whether that is for trade or for purposes of criminal investigation online and offline. Transatlantic cooperation on cyber issues and the TTIP were profoundly affected by the Edward Snowden revelations that exposed wide-ranging 'mass' surveillance by US intelligence agencies of European citizens and

elites and which fundamentally dented the trust between the US and EU in their collaborative efforts. Moreover, it has brought to the fore and accentuated the differences between the US and the EU on the issue of the right balance between data protection and privacy and information and intelligence sharing (and gathering) in order to ensure effective and resilient cybersecurity.

This is not to say that the US and the EU are fundamentally culturally incompatible when it comes to partnership, collaboration and cooperation in relation to cybersecurity and cybercrime. Clearly this is not the case as they still hold similar views on global Internet governance – a free, open, secure, accessible Internet for all – and on the need to develop effective mechanisms to combat cybercrime and protect and make resilient critical industry information infrastructure. Furthermore, platforms have been established for closer cooperation between the EU and US on cybercrime and cybersecurity – such as the Working Group created in November 2010 that focused on: (a) cyber incident management; (b) public-private partnership; (c) awareness raising; and (d) cybercrime, out of which was launched the Global Alliance against Child Sexual Abuse Online (December 2012). In the post-Snowden era, and one might argue a subsidence with regard to the initial anger surrounding mass surveillance, the EU–US dialogue on cross-cutting and foreign policy related issues was established (March 2014) as well as an Information Society Dialogue to focus on broader cybersecurity related issues including Internet policy and governance.

However, whilst certain progress has been made in the post-Snowden era there is no doubt that the disclosures regarding National Security Agency (NSA) espionage activity had an adverse impact on the evolution and progression of a transatlantic partnership and culture of cybersecurity and resilience based on trust and a shared understanding of the problem and solution with regards to the logics and laws for cybersecurity. In this context this chapter will focus on and analyse the EU–US relationship and its implications for the EU in developing the transatlantic dimension of its cybersecurity strategy and ecosystem. More specifically, it will analyse similarities and differences between EU and US logics of security across different issues related to security in cyberspace. The first section will focus on the broader issue of Internet governance and the challenge for the EU–US partnership with regards to alternative proposed models of Internet regulation and security. The second section will then analyse in detail the implications of Snowden and specifically, US and EU approaches to cyber cooperation (cultures of cybersecurity) and what this means for the emergence of an effective

transatlantic security as resilience. The third section will assess progress made through the relevant established formal and informal arrangements between the EU and US with regard to combating cybercrime and constructing an effective transatlantic cybersecurity of resilience. The final section will assess the extent to which the EU–US partnership can foster the necessary conditions for an effective security as resilience to emerge between two key global players and more broadly, in relation to the evolution of a global cybersecurity ecosystem of resilience.

Governing cyberspace

The EU and the US have similar normative positions on the Internet and how it should be governed, even though historically and following the Snowden revelations there have been moments of disagreement and contention, with the EU calling for greater inclusiveness and transparency within the global fora – in particular the Internet Corporation for Assigned Names and Number (ICANN)[1] – that regulate the Internet. They both subscribe to the principle of a global Internet that is fundamentally a public, collective good and from this that the Internet should be available to and accessible by all citizens. Thus they share a normative view of an Internet with no restrictions or limitations, the exception to this rule being the use of instruments for preventing harm to others in the online environment (Christou 2014).

The EU and US also share similar views on the model for regulating the Internet, ensuring that rights online are protected and that the Internet is secure and accessible so that economic benefits can be maximised. Such a multistakeholder model was born from a long, controversial and contested process – the UN World Summit on the Information Society (WSIS 2002–2005) – throughout which challenges to US unilateral control of the Internet emerged. Such a challenge came from the EU that wanted more intergovernmental oversight within ICANN; that is, a change in the nature of the public-private relationship originally constructed (Christou and Simpson 2007, p.154–156). It also, more saliently, came from those states such as Russia, China, Saudi Arabia and Iran that preferred a multistate model and a complete shift away from 'all stakeholders' to governmental control of Internet governance and regulation through the UN in order to dilute US control (Laprise 2014).

The Working Group on Internet Governance (WGIG) that was established by then UN Secretary-General, Kofi Annan, to define Internet governance and the structures and responsibilities of actors within it, ultimately supported – in the face of US refusal to give up control and

ownership of the Internet – the creation of a forum that would provide 'a space for dialogue for all stakeholders on an equal footing on all Internet Governance issues' (WGIG 2005, p.10). This culminated in the idea of the Internet Governance Forum (IGF) that although formed under the auspices of the UN, was a body that would allow stakeholders to come together to discuss, deliberate and come up with solutions to, all issues related to Internet governance. Since then the multistakeholder model, embodied not just within ICANN and the IGF, but also standard setting and regulatory bodies such as the Internet Engineering Task Force (IETF), has been upheld as the normatively right model for Internet governance – including security – given the nature of the Internet and the potential impact it can have on a variety of stakeholders. Indeed, evidence of best practice discussed at the IGF has been diffused into domestic policies (Christou and Simpson 2012), ICANN structures and programmes have demonstrated how practical issues can be resolved within its inclusive process, and in general the multistakeholder approach has ensured the maintenance of an open and free Internet that has allowed innovation and diversity to prosper (Bendiek 2014, p.8).

This model, of course (as shown in Chapter 3), is not without controversy and has been challenged at every opportunity by those states that want to see greater state control and a more intergovernmental approach to Internet governance; and that have expressed concern over US control and oversight of the management of the Internet (ICANN). At the World Conference on International Communications (2012), for example, convened to revise Internet Telecommunications Regulations (ITRs), there was a proposal by Russia, China, Saudi Arabia, Algeria and Sudan that sought to extend ITR jurisdictions. That is, sovereign state control over all aspects of Internet governance, including security aspects. Although such a proposal was eventually withdrawn, the ITU adopted a compromise non-binding resolution (Resolution 3) included in the final ITR text that effectively embedded the language of intergovernmentalism and greater state control over Internet related technical, development and public policy issues (Kruger 2013, p.12). The result was that the US refused to sign the final treaty, particularly because of the implications that this might have for subsequent ITR articles on cybersecurity and cybercrime; but as Klimburg suggests, 'the wider implications of the [final] document could well be a "semantic beachhead" with which to further attack the issue of multistakeholderism' (2012, p.4).

Whilst sure enough, fora such as the ITU WCIT in 2013, saw similar challenges to the multistakeholderism model, the EU and the US (and an alliance of other Western states) have consistently defended it – and the principles of a free and open Internet. However, Edward Snowden's release of classified US documents in the summer of 2013 that revealed the scope of US intelligence surveillance activities was a moment in which the solidarity within the Western alliance – and particularly between the EU and US – was questioned, with certain implications for transatlantic cyber collaboration. Even prior to the Snowden revelations the EU had consistently called for greater accountability and transparency and a more equal role for the Governmental Advisory Committee (GAC) with regards to the oversight and functioning of ICANN (European Commission 2009), whilst supporting multistakeholderism in principle (Christou and Simpson 2011). Though the US, through the Affirmation of Commitments (2009) signed by ICANN and the US Department of Commerce indicated a commitment to periodically review the four core objectives of ICANN – including that of accountability, transparency and the interests of global Internet users, this did not result in the reduction of US unilateral oversight over ICANN and the Internet Assigned Names Authority (IANA) function. Thus after Snowden, the EU went a step further in also demanding greater inclusivity for democratic states such as Brazil and India, and in challenging more assertively the unilateral power of oversight of the US in ICANN.

To this end the European Commission – led by DG Connect – established the Global Internet Policy Observatory (GIPO), with the objective of creating a more inclusive and transparent technical platform for participation in Internet governance. GIPO was established in cooperation with not just like-minded countries such as Brazil, India and Switzerland, but also regional organisations such as the African Union, as well as certain non-governmental organisations. The purpose then was to ensure that all stakeholders – even those with limited resources – could have greater access and participate in, through a technological solution, Internet governance policy-making processes, information and discussion.[2] Thus GIPO's aim is not to displace existing fora and platforms for Internet governance discussions, but rather, give further voice and influence to those emerging democratic powers and regional organisations that want to challenge US control over the functions of the Internet (Interview, DG Connect official, March 2013).

Furthermore, the EU reiterated its commitment to transparency and inclusiveness at the Multi-Stakeholder Meeting on the Future of Internet

Governance (NETmundial) held in Sao Paulo, Brazil (April 2014) and the IGF meeting in September 2014. Indeed a common and consistent projection and message from Neelie Kroes, former Vice President of the European Commission and member of the High-Level Multistakeholder Committee of NETmundial, was to ensure the globalisation of IANA and ICANN as well as strengthening the IGF and improving the multistakeholder model for Internet governance. The very rationale for this position was articulated clearly by Kroes: 'Recent revelations of large-scale surveillance have called into question the stewardship of the US when it comes to internet governance . . . Given the US-centric model of internet governance currently in place, it is necessary to broker a smooth transition to a more global model while at the same time protecting the underlying values of open multi-stakeholder governance . . . Large-scale surveillance and intelligence activities have led to a loss of confidence in the internet and its present governance arrangements.' (Kroes cited in Traynor 2014). NETmundial produced a document, in the end, that set out common principles and values for an inclusive, multistakeholder and evolving governance framework for the Internet – with a roadmap on how to achieve this which both the EU and the US have committed themselves to achieving (Press release, 1st EU–US Cyber dialogue 2014).

In this context the US, in March 2014, announced its intention to set forth a process that would see the National Telecommunications and Information Administration (NTIA) relinquish its oversight function in relation to ICANN, but with two major caveats: 1. That the current system of oversight is replaced with a multistakeholder model not dominated by states 2. That the current system and structures that support it remain in place until any new governance mechanisms are agreed by the internet community. This had the dual effect of: placating those, such as the EU and its member states, with regard to the 'surveillance' for 'security' debate that emerged with the Snowden revelations and subsequent issues of US control of the Internet for its strategic interest; whilst also ensuring that it sustained a consensus among like-minded states and organisations (NGOs, regional organisations and so on) on the values that should underpin the governance of the Internet – and importantly, the broad array of actors that should participate in such processes. The alternative 'sovereignty' based vision of Internet governance articulated by states such as Russia and China was thus, temporarily at least, discredited, with the potentially more inclusive 'transitional' mechanisms the main focus of deliberations in subsequent international fora. It also meant that the EU and other like-minded emerging democracies had

a basis on which to pressure the US government into realising the momentum and creating concrete structures for a more inclusive Internet governance, even if, at the time of writing, the US government remains *in* control of the Internet's main functions.

Security, data privacy and data protection

A key obstacle to cooperation in cybersecurity is the cultural challenge posed by interaction in such a complex technical and legal domain. It can be argued that the mass surveillance and monitoring programmes such as PRISM (as well as others such as Bullrun, Upstream and so on) carried out by the US and its intelligence agencies, served to exacerbate the different approaches to securing cyberspace advocated by the EU and the US, and therefore simultaneously hinder collaboration but also catalyse a reflective process through which it could be effectively restored.

EU and US logics and approaches

The tension between the US and EU on the balance between security and data privacy stems and is underpinned by the fact that cybersecurity policy is driven by different logics for each. The EU approach has been characterised as legalistic focusing on cybercrime, with an emphasis on cyber defence and soft power capabilities (Bendiek 2014; Christou 2014). Indeed some have even gone as far as describing the EU as a civilian cyber power (Dunn Cavelty 2013). The EU, as highlighted in previous chapters in this book, is predominantly focused on constructing a resilient ecosystem that enables not only protection through building capacity, but also the ability to bounce back and recover from cyber attacks. Moreover, the EU's approach has embedded within it the notion of security as resilience (essentially Type 3 resilience – see Chapter 2) where security does not mean the ability to build offensive capacity and defend the cyber perimeter, but rather adheres to the notions of creating adaptable, flexible and robust systems and a complex regulatory environment that is characterised by shared responsibility and multiple stakeholders. Building resilience then, is the driver for ensuring more effective cybersecurity in Europe; and such an approach – at the level of the EU at least, if not all EU member states – is not driven by a security logic that prioritises data collection for 'security' no matter what the implications for abuse of power, civil rights and ultimately the security of the citizen (Ibid., p.8; Bigo et al. 2013; Bowden et al. 2013; Coaffee and Fussey 2015).

In contrast, the US approach to cybersecurity has at its very core the concepts of military defence (which includes offence in contrast the EU) and deterrence (Lewis 2014; Sofaer et al. 2010), and encompasses a wide range of priorities and principles (see Box 7.1).

Box 7.1 US cybersecurity priorities

Priorities

1. Protecting the country's critical infrastructure – our most important information systems – from cyber threats.
2. Improving our ability to identify and report cyber incidents so that we can respond in a timely manner.
3. Engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.
4. Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets.
5. Shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.

Principles

1. Whole-of-government approach
2. Network defense first
3. Protection of privacy and civil liberties
4. Public-private collaboration
5. International cooperation and engagement

Source: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

Despite this, however, such priorities are driven by the dominant perception of cybersecurity as a threat to national security; a threat that can be most effectively addressed by enhancing, through military means, US hard power in cyberspace (Bendiek 2014, p.17; Stevens 2012).[3] For example, the Centre for Strategic and International Studies' Commission on Cyber Security in its report (2008) portrayed cybersecurity as 'a major national security problem' for the US. In what subsequently followed, President Barack Obama's overhaul of US cybersecurity policy

led to a reorganisation of cyber defence capability and strategy through the Department of Defence (DoD), a move which increasingly equated cybersecurity to military security and which included the notion of pre-emptive attacks.

This move was also reflected in the institutional location of cyber defence responsibility, when previous task forces were consolidated into the US Cyber Command (USCYBERCOM) which in turn reported to US Strategic Command (Porcedda 2012, p.48). The central tasks of USCYBERCOM were twofold: 1. Computer Network Defence (to coordinate defence operations against cyber attacks); 2. Cyber Attack Operations (to build and enhance offensive cyber attack capability). Indeed, on the latter, and given the increased projection (and perception) of cyber risks posed by actors outside the US (for example, Chinese cyber espionage), the US International Strategy for Cyberspace (2011) states quite unequivocally that 'When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat'. Importantly then, the US strategy of defence and deterrence was based on the ability to create a climate of fear among cyber enemies through increased militarisation (capacity and strength). This is despite the fact that any logic of deterrence also implies clear lines of 'attribution' and based on this, retaliation; which is not always feasible or possible in cyberspace given that technical protocols guarantee a certain amount of anonymity for users. Indeed even if attribution was less complex, the issue of what is proportionate and appropriate in retaliation against cyber attacks is still controversial even though the Tallinn Manual (2013) has sought to sketch out the rules of cyber warfare.

As well as institutional transformation a considerable amount of resource – human and financial – has been made available to meet USCYBERCOM objectives. For example, the head of USCYBERCOM and the US National Security Agency (NSA), General Keith Alexander, has been developing over the last two years 40 new teams of cyber agents, 13 of which will focus on offensive cyber attacks against other countries and cyber adversaries. In short, such teams have been described by Alexander as 'defend-the-nation' teams that are 'analogous to battalions in the Army and Marine Corps – or squadrons in the Navy and Air Force . . . they will soon be capable of operating on their own, with a range of operational and intelligence skill sets, as well as a mix of military and civilian personnel' (Pentagon creates 13 offensive cyber teams 2013). The numbers employed with USCYBERCOM have also increased fourfold since its launch (to just under 5,000), with the financial resource for cybersecurity also increasing year on year to support

actions across the US government. For example, in 2013 the budget for cybersecurity was $52.6 billion – with an addition $14 billion being requested for the 2016 fiscal year (Obama seeks $14 billion to boost US cybersecurity defences 2015). Two thirds of the budget since 2013 have been requested and spent by the Central Intelligence Agency (CIA), the NSA and the National Reconnaissance Office (NRO) (Bendiek 2014, p.16). Indeed the Pentagon alone in 2016 requested $5.5 billion in funding for 2016 ($4.7 billion in 2014).

Practices flowing from the above offensive logic and resource to support it have also spilled over into the intelligence dimension, and have had serious ramifications with regards to the issue of how data has been collected and utilised by the US government and its agencies for the purpose of addressing the national threat that cybersecurity poses. For example, the US intelligence community regularly engage in offensive cyber operations – a total of 231 in 2011 according to leaked (Wikileaks) documents, with other funded projects being specifically employed to penetrate foreign networks through placing 'covert implants'; sophisticated malware in computers, routers and firewalls (Gellman and Nakashima 2013). There are also plans in the next phase of offensive cyber-operations for US spy agencies to use an automated system called TURBINE that can manage millions of implants for gathering intelligence and actively attacking machines (Chan 2013). Furthermore, it has been argued that the NSA has bought and exploited 'so-called zero-day vulnerabilities in current operating systems and hardware to inject NSA malware into numerous strategically opportune points of Internet infrastructure' (Dunn Cavelty 2014; Greenwald and MacAskill 2013). In addition, it has also been revealed that US government resource deployed to crack existing encryption standards has contributed further to the very vulnerability of those encryption systems (Dunn Cavelty 2014; Clarke et al. 2013).

Such activities, it can be argued, have serious implications for achieving security as resilience – and sit in direct contrast to the logics underpinning EU cybersecurity (but not necessarily certain EU member states). They do not only create a market (and incentive) for producing and selling such vulnerabilities; these backdoors or sleeper programs can be used at any time for different purposes (disruption, surveillance and so on), and can ultimately lead to further insecurity and vulnerability whilst also impacting on trust and confidence in cyberspace. As Dunn Cavelty (2013, p.9) points out, those that insert the backdoors, cannot guarantee that they remain in control of them and thus could quite feasibly be exploited by the very cyber criminals, hackers and terrorists

that such measures seek to protect against. Such practices, driven by a national security logic, can increase the threat for states and citizens alike; and adversely affect the resilience of any ecosystem through the direct and indirect creation of vulnerabilities.

Network and information security: Critical infrastructure protection

Whilst in relation to cyber defence, EU–US logics are fundamentally different, on the issue of Network and Information Security (NIS) – and in particular critical infrastructure protection (CIP), there is at least some sense of convergence on the need for regulation and a more hands-on meta governance with regard to reporting – even though there has been resistance to a mandatory approach both in the EU (see Chapter 6 for details) and in the US.

In the EU, ENISA continues to highlight in its annual threat landscape reports (ENISA Threat Landscape 2013, 2014) the risks associated and potential consequences of cyber attacks on critical infrastructure.[4] The NIS Directive (see Chapter 6) is still under discussion at the time of writing in the EU Council of Ministers after being agreed by the European Parliament in March 2014. However, whatever the agreement in the Council the final version is likely to be much narrower in its focus in relation to the sectors and market operators included with regards to mandatory reporting of incidents; mainly due to a number of amendments made by the Internal Market and Consumer Protection Committee (IMCO) of the European Parliament (Pearse et al. 2015; Long 2014). Moreover, member states are likely to have much more discretion on whether to include public administrations within the remit of the Directive – thus potentially opening up more avenues for voluntary arrangements between government and the private sector. Thus whilst the NIS Directive will no doubt provide for the establishment of NIS competent authorities in EU member states which will monitor compliance with the Directive, promote NIS strategy and receive, collate and share information on cybersecurity attacks and threats, the flexibility in interpretation and reduced scope of the Directive might have an adverse effect on the quality of the institutions established, and the consistency and sharing of reliable information.

In the US, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and organisations such as the National Research Council (NRC) have reported on the increasing number of cyber attacks on critical infrastructure and speculated extensively on the potential impact they could have. According to some scholars, this has

heightened the sense of urgency among certain US government organs to be more proactive in establishing measures for the protection of national critical infrastructure – including, and in particular with regard to the relationship with the private sector (Titch 2013, p.3). However, there has also been significant resistance from business, civil rights and Internet privacy advocates and different parts of the US government on proposed legislation (see below). The result has been reliance, in the US, on a voluntary 'market' and 'hands-off' meta-governance approach to information sharing between government and critical national infrastructure providers, despite efforts to introduce mandatory reporting.

To elaborate further, on several occasions over the past few years bills have been introduced to Congress that would facilitate the mandatory sharing of information on cyber threats and attacks between the US government and relevant private sector infrastructure providers. The Cyber Intelligence Sharing and Protection Act (CISPA), for instance, was put forth on 30 November 2011 (with 111 co-sponsors), and although it was passed by the House of Representatives by a majority vote in April 2012, it failed in the US Senate, amid fears that it would eventually be vetoed by the White House because it lacked sufficient safeguards with regards to civil liberties and confidentiality but also because it did not go far enough in terms of incentivising the adoption of cybersecurity standards and protocols by the private sector. Many questioned how far such a bill would be compatible with laws that did provide such safeguards, such as the Electronic Communications Privacy Act (ECPA) (Titch 2013, p.4–10). Despite the bill being reintroduced in 2013, 2014 (as the Cybersecurity Information Sharing Act) and 2015, no outcome was secured and at the time of writing (March 2015) it had been referred to the Committee on Intelligence in order to assess whether it should be brought to the House for a vote once again.

Precisely because attempts to pass the above bill failed, an Executive Order (13636) was issued by the President of the US, Barack Obama, in February 2013 that sought, as one of its core objectives, to construct a voluntary Framework and Roadmap for Improving Critical National Infrastructure Protection.[5] That is, rules that would guide information sharing between the US government and owners and operators of critical infrastructure and that would facilitate (incentivise) the implementation of minimum cybersecurity standards. The National Institute for Standards and Technology (NIST) was responsible for launching the Framework in February 2014, and developing a cost-effective way 'to reduce cyber risks to critical infrastructure' (Pearse et al. 2015). Moreover, the NIST, alongside the Department of Homeland

Security (DHS) and the Department of Defence (DoD), were all tasked with creating a partnership with the owners and operators of critical national infrastructure through, in addition to creating a cybersecurity framework:

- New information sharing to provide classified and unclassified threat and attack information to US companies.
- A voluntary program to promote the adoption of the framework
- Review of existing cybersecurity regulation
- Strong privacy and civil liberties protections based on the Fair Information Practice Principles

(EO 13636: Improving Critical Infrastructure Cybersecurity 2014)

As with the original European Commission proposed EU NIS Directive the scope of the US framework is broad, including a wide range of sectors, and indeed incentives to adopt the Framework across these sectors, such as cybersecurity insurance, grants and cybersecurity research. Such policy ideas have also appeared in the EU cyber strategy and in the strategies of leading member states such as the UK, albeit in different forms. In this sense then, there is a similarity in approach between the Obama administration and the EU in terms of the desire for the implementation of minimum cybersecurity standards and incentivising adoption of such standards as well as information sharing. Indeed there is also agreement that the approach taken should be underpinned by legislation and regulation – the key difference, of course, being that in the US this has been continuously resisted by the Senate and other critical voices, whereas in the EU, the mandatory obligation to report is embedded in the NIS Directive (despite certain scepticism from leading member states), even if the final form might well reduce the scope and reach of it. Whilst this indicates some convergence in thinking on the issue of how to enhance cyber resilience between the US and EU in relation to CIP, it might also be argued that if these approaches result in different practices – this could also lead to inconsistencies in reporting and therefore responses to potential cyber threats given the global nature of cybercrime. Moreover, the debate in the US on a mandatory approach to information sharing demonstrates the sensitivity of such an issue with regards to the rights of US citizens – but also importantly, the potential differences between the EU and the US on the relationship between privacy, freedom and security given the logics within which such issues are addressed.

Data privacy and protection

The conversation between the EU and the US on data privacy has been described by some as 'uneasy' given the difference in attitudes, culture and legal systems; with this difference being acutely exacerbated by the Snowden disclosures (Kerry 2014; see also Bygrave 2013). This said, equally uneasy are the conversations between EU member states with regard to the relationship between security and data privacy. Some, such as the UK (GCHQ) were complicit in NSA surveillance activity highlighting the disagreements within the EU over when and how data for security and counter-terrorism purposes should be collected, stored and utilised.

Such activities were singled out and condemned by the European Parliament's civil liberties committee report on mass surveillance. Indeed there was criticism of mass surveillance not just in the UK and the US, but also France, Germany and Sweden – and in particular the clear lack of competence on the part of oversight committees across EU countries to provide any sort of accountability – at the political (democratic legitimacy) or technical level (installing back doors and not fixing vulnerabilities) (European Parliament 2013; see also Bigo et al. 2013). The European Commission, and in particular Vivienne Reding, Vice-President and Commissioner for Justice, Fundamental Rights and Citizenship at the time of the Snowden revelations (June 2013), was also clear in the message that 'such activities have grave adverse consequences for the fundamental rights of EU citizens' (Reding 2013), and that there could be no compromise on standards of protection enjoyed by European citizens going forward. Whilst there was recognition by Reding that national security was a matter for EU member states, the Snowden case demonstrated that a clear legal framework for the protection of personal data was not a luxury but an absolute necessity and fundamental right for all EU citizens (cited in Watt 2013). Indeed, Reding went as far as advocating the development of a European cloud[6] as an alternative for ensuring the security of European data (see Venkatraman 2013).

The mass surveillance security practices of the NSA, authorised by the US administration, were justified by a 'national security' logic, and a body of US law, underpinning the US approach to cybersecurity. The Report of the ad hoc EU–US Working Group on Data Protection (2013) highlighted the US legal basis on which surveillance activities were carried out. There were two fundamental elements to this that allowed for the collection of personal data by US intelligence agencies: the first

was Section 2 of the Foreign Affairs Surveillance Act (FISA); and the second, Section 215 of the USA Patriot Act 2001. Under these laws authorisation and oversight of intelligence collection is provided by the FISA court. Other provisions also allow for the collection of foreign intelligence information – such as the Executive Order 12333 – for which there is no judicial oversight but where activities pursued under this 'Order must not violate the US Constitution or applicable statutory law' (Ibid.). The US Constitution, in this instance, does provide protection for US citizens on data collection under the Fourth Amendment – which prohibits 'unreasonable searches and seizures' and requires that a warrant must be based upon 'probable cause'. However, this protection does not extend to non-US nationals unless they have become or are part of the US national community; raising the question of how well protected the data of European citizens is when using US online services.[7] The sharing and use of citizens' personal data in the US is also protected by a host of laws across different sectors – and enforced by the Federal Trade Commission if companies are found to violate their privacy policies (Kerry 2014, p.2).

The NSA revelations raised ethical as well as legal questions on the balance between privacy and rights – in the US and the EU – and indeed, the extent to which US authorisation of the surveillance of European citizens and heads of government – was necessary and proportionate to meet the interests of national security (European Commission 2013e; Bendiek 2014, p.20). In other words, it raised the issue of whether EU and US 'cultures' of cybersecurity were compatible when it came to personal data collection and its use for intelligence purposes, given the logics that underpinned the approaches taken. This in turn provided added momentum to ongoing reforms on data privacy and protection in the EU (the EU's 1995 Data Protection Directive) and US (the Consumer Privacy Bill of Rights) and catalysed a series of new reviews on existing rules and transatlantic agreements on data flows that sought to restore and ensure rights and most importantly, rebuild trust.

One such agreement was that of Safe Harbour (European Commission 520/2000/EC), which was put in place in order to ensure adequate protection for the purposes of personal data transfers from the EU (European Commission 2013d, p.2). The agreement essentially provided principles (see Box 7.2) for protecting privacy that had to be adhered to, through self-certification, by US companies transferring data on EU citizens; and whilst signing up to such arrangements was voluntary, adherence to the rules if signed up was not. The review of Safe Harbour conducted by the European Commission in 2013 revealed that many of the 3246 companies signed up to Safe Harbour were not complying with

the obligations of the agreement (Ibid., p.4), and increased violation of such principles over time was also confirmed by other independent reports (see Bendiek 2014, p.21). The reforms suggested by the Commission, however, were considered to be moderate given the initial calls by the European Parliament to suspend Safe Harbour, and Vivienne Reding's rhetoric on Safe Harbour as a potential loophole undermining EU protection laws (Alden 2014).

Box 7.2 Safe harbour: Basic overarching principles

1. Transparency of adhering companies' privacy policies
2. Incorporation of Safe Harbour principles in companies' privacy policies
3. Enforcement, including by public authorities

Source: European Commission (2013d, p.2).

The main recommendations for strengthening the Safe Harbour Privacy Principles, in this context, centred on: making alternative dispute resolution more available and accessible (affordable) to individuals; ensuring onward protection of data when transferred to a third party processor; greater transparency of Safe Harbour companies' privacy rules and in particular whether data can be collected from them under US laws and regulations; enhancing processes and tools for enforcing Safe Harbour Principles (European Commission 2013d, p.14–19). Given the importance of the agreement, and the adequacy of its provisions on data flow and privacy to the parallel negotiations on TTIP, such recommendations have been criticised as deficient by some, but sufficient 'to improve the functionality of Safe Harbour', by the Commission (Reding cited in Saran 2014). From a US position data flows is an issue for negotiation in TTIP – but from an EU perspective, it has been omitted from the agenda precisely because high levels of data protection and rights of privacy are a non-negotiable part of TTIP; a clear obstacle to future cooperation if agreement cannot be reached on the interoperability of privacy and data protection systems.

Whilst Safe Harbour is an agreement that applies specifically to economic and trade dimensions of data flow and protection, the implications, as indicated above, are much broader (that is, cooperation in criminal matters) given the question of how much access the US government has to data stored by private companies, many of which

operate transnationally. This is also the case with the EU's proposed draft of the General Data Protection Regulation (GDPR), the purpose of which is to enhance and harmonise data protection standards throughout the EU, and to provide additional safeguards, rights and enforcement processes when European data is being used inside or outside the EU[8] (GDPR 2014). The GDPR and its negotiation was controversial – with the European Parliament (EP) introducing (post-Snowden) an anti-FISA clause (Bendiek 2014, p.21) and so-called Article 42 that would have put a sunset on Safe Harbour (Kerry 2014, p.4).

Whilst these did not appear in the final version agreed by the EP in March 2014,[9] intense lobbying meant that no less than 3999 amendments were made to the original Commission proposal (January 2012) by the Civil Liberties, Justice and Home Affairs Committee (LIBE). The agreed version, at the time of writing (March 2015), is still under discussion in the Council of Ministers, with critical issues (among others) such as the right to erasure, informed consent and transfer of data to third countries still to be resolved. Such issues have proved to be controversial throughout the process – with, for example, the issue of transferring data to third parties and countries deleted from the original Commission proposal after intensive lobbying by the US government, only to be reinserted by the EP in the final agreed version. Member states have not incorporated this approach into their version thus far, and if omitted would fundamentally weaken the rights of European citizens with regard to data use and transfer. Similarly on the issue of informed consent – whilst the Commission and final EP version insist on explicit consent – that is, individuals being able to consciously agree or disagree on what happens to their data, member states have thus far leaned towards a 'more vague "unambiguous" consent', which for some 'would give a cheap excuse to data controllers', not to ask for consent, thus lowering the level of protection from that originally proposed (Albrecht 2015).

The EU and US have in addition, specific agreements on the use and transfer of data in police and judicial matters, with negotiations ongoing on an 'umbrella agreement' in this area with the objective of 'ensuring a high level of data protection, in line with the EU data protection acquis, for citizens whose data is transferred across the Atlantic, thereby further strengthening EU-U.S. cooperation in the fights against crime and terrorism' (European Commission 2013e). Debates and disputes emerged over levels of personal data protection prior to and in particular after the Snowden revelations on the Passenger Name Record Agreement (PNRA) (the transfer of flight information) the Terrorist Finance Tracking

Program (TFTP) (exchange of financial data through the SWIFT system) and the Mutual Legal Assistance Agreement (MLA) (facilitating the exchange of information and evidence in criminal cross-border investigations). In essence, the negotiations for the umbrella agreement, for the EU, entailed securing the same level of data protection offered in the GDPR for data transfer in police and judicial cooperation on criminal matters (European Commission 2013d).

Central to this has been ensuring that EU citizens not living in the US have the right to judicial redress and benefit from the same safeguards as US citizens. In the context of increasing US public scepticism and the economic consequences of mass surveillance for security, the Obama administration took 'the unprecedented step of extending certain protections . . . for American people to people overseas' (Kerry 2014, p.10) recommending that the US Privacy Act (1974) be revised in order to include non-US nationals. However, in practice, this commitment has not yet resulted in a practical solution through legislation in Congress. Moreover, even if an adequate mechanism is found for granting judicial redress to EU citizens in the US, for some, 'this will not bring to an end – or even bring transparency to – the wholesale violations of EU citizens' rights by US surveillance via its top secret intelligence programmes' because the Privacy Act of 1974 is subject to exceptions and does not cover data collected for the NSA and other national security programmes (Micek and Masse 2014). In addition, agreement has not been reached on the critical issue of limiting data transfer to specific law enforcement purposes, which would then also be processed for these purposes only (European Commission 2014).

This said, certain reforms stemming from President Obama's requested review of Intelligence and Communication Technology (for the Report see Clarke et al 2013) have been instigated, including the 'declassification of FISA court decisions and other intelligence materials', which for some, has provided for more transparency around foreign intelligence collection by the US (Kerry 2014, p.10). Other measures have included limitations on the collection and use of data, strengthening civil liberty and privacy protections under Section 215 of the US Patriot Act and Section 702 of the FISA, as well as providing further mechanisms for the protection of whistle-blowers (Office of the Director of National Intelligence 2015). In addition, a Big Data Working Group was set up led by Counsellor to President Obama, John Podesta, which also made commitments to advance the Consumer Privacy Bill of Rights in the US; making it legally enforceable by the Federal Trade

Commission in order to provide a more solid foundation of trust by 'establishing a broad set of principles for businesses and consumers' (Ibid., p.17).

Progress then has been made on both sides of the Atlantic on the reform of privacy and data protection systems – and though it seems the EU and US don't disagree on key values for IG, there is still some way to go when it comes to cultural and legal aspects of cybersecurity. However, whilst the EU's underlying logic to cybersecurity allows for a more legalistic, regulatory, rights-based approach at the European level, individual member states (the UK, Germany, France, Sweden) clearly, alongside the US, also take a 'national security' first approach on this issue of data collection for criminal matters, making the relationship between citizens' rights and governmental security objectives as problematic in Europe as in the US when it comes to constructing an effective transatlantic security as resilience. Even EU legislation such as the E-privacy Directive (2009) allows personal data to be used for 'crime prevention' and other purposes, thus providing a weak framework for individual data protection where the national security logic is primary (Bendiek 2014, p.23). Indeed even though the Data Retention Directive (2006) was declared invalid by the European Court of Justice in April 2014, precisely because it constituted a 'serious interference with . . . the right to privacy and the right to protection of personal data' (Villalon cited in Hern 2014) – member states such as the UK have continued to enforce the Directive to ensure access to communications data[10] (Ibid.). Moreover, such a judgment also impacts on the nature of data collection within already existing EU–US mechanisms such as PNR and TFTR – and in particular the way in which undifferentiated bulk data has been transferred to US authorities – that is, data of unsuspicious individuals with no clear link to being a public security threat. This in turn, has implications for the fundamental rights of such individuals and the way in which the EU and US collect data for security purposes (see Boehm and Cole 2014). Finally, the tensions between individual rights and security logics also stretch to international level – where the Budapest Convention (cybercrime) and the Tallinn Manual (cyber warfare) do not provide clear guidelines for the protection of personal data and the rights of individuals (Bendiek 2014, p.23).

EU–US platforms for cooperation and coordination on cybersecurity and cybercrime

The US-EU fact sheet (2014) on cyber cooperation between the two partners highlights the extent to which 'cooperation is founded on

our shared values, our interest in an open and interoperable Internet, and our commitment to multistakeholder Internet governance, Internet freedom, and protecting human rights in cyberspace. International cyberspace developments are central to our broader foreign and security policy, and are key elements of our strategic partnership'. However, given the context already alluded to above, it is pertinent to ask how the similarities and differences between the EU and US on the various facets of cybersecurity and cybercrime have actually resulted in effective platforms for cooperation and coordination? More importantly, it is critical that we understand the extent to which this has resulted in a more effective security as resilience in any joint endeavours undertaken.

There has certainly been no shortage of initiatives in the past five years that have sought to enhance efforts on this front, the first of these established in the context of the 20 November (2010) EU–US Lisbon Summit in order to 'enhance cybersecurity and cybercrime activities and contribute to countering global cybersecurity threats'. The Working Group on cybersecurity and cybercrime established a clear set of objectives and priority areas, as well as specific deliverables, with the aim of annually reporting on progress made within each. The four main areas were: Cyber incident management; Public-Private Partnerships; Awareness Raising; and Cybercrime (EU–US Working Group, Concept Paper 2011). Whilst it is clear that the Snowden revelations had a negative impact on many aspects of work that the Working Group – and the expert sub groups (to address one each of the above main areas) were set up to do, some progress and concrete outcomes did emerge from it (Interviews, European Commission, June 2013).

For instance, public-private workshops on industrial control systems have been hosted and both partners have jointly promoted National Cyber Awareness Month in the U.S. and Europe (US-EU fact sheet 2014). The EU and US also conducted a transatlantic cybersecurity exercise as well as organising the exchange of information on national and regional cyber exercises. The bilateral table top exercise, Cyber Atlantic, was conducted in November 2011, with the purpose of determining how the EU and US could cooperate effectively (see Box 7.3 for objectives of the exercise). This was the first (and only) joint exercise undertaken by the EU and US – and was therefore exploratory in nature. Nevertheless over 60 participants from 16 EU member states took part as well as representatives from the US government, and it was facilitated by the European Network and Information Security Agency (ENISA) on the EU side and the Department of Homeland Security (DHS) in the US. Unfortunately,

no documentation (report) is available publically on the lessons learnt and outcomes from this exercise due to the sensitivity of the issue, and it seems that the politics of Snowden, as well as separate bilateral EU member state engagement and collaboration with the US, has meant that progress with regard to the Commission directed Cyber Incident Management programme has been very slow (Interview, ENISA official, March 2015).

Box 7.3 Cyber Atlantic (2011) objectives

To explore and improve the way in which EU Member states would engage the US during cyber crisis management activities

To explore and identify issues in order to improve the way in which the US would engage EU Member states during their cyber crisis management activities, using the appropriate US procedures;

To exchange good practices on the respective approaches to international cooperation in the event of cyber crises, as a first step towards effective collaboration.

Source: ENISA, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011.

Beyond cyber exercises, the Global Alliance against Child Sexual Abuse Online, launched in December 2012, was a successful product of the work of the EU–US Working Group (Interview, European Commission, June 2013). This international collaborative partnership, made up of 54 countries[11] (A Global Alliance against Child Sexual Abuse Online 2015), set out four shared policy targets (see Box 7.4) with the aim of fighting the growing threat to children online. To this end, much positive progress was made in meeting the targets, but significant obstacles and challenges still exist to constructing a more effective security as resilience in relation to the operational, legal and technical as well as technological dimensions (Report of the Global Alliance 2013, p.3; Ministerial Declaration 2014). Thus, plans have been outlined by the countries signed up to the agreement that demonstrate their commitment to achieving the set targets, and which speak to improving

coordinative, collaborative and technological tools and mechanisms, as well as enhancing skills, training and institutional platforms that will further enable the fight against child sexual abuse online.

Box 7.4 Global Alliance against Child Sexual Abuse Online: Shared policy targets

1. enhancing efforts to identify victims and ensuring that they receive the necessary assistance, support and protection;
2. enhancing efforts to investigate cases of child sexual abuse online and to identify and prosecute offenders;
3. increasing awareness among children, parents, educators and the community at large about the risks;
4. reducing the availability of child pornography online and the re-victimization of children.

Source: European Commission http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm.

Some pertinent examples, include, plans to improve the use and content of INTERPOL's International Child Sexual Exploitation database (ICSE), through expansion of access for Alliance country members and their contribution to it. For the US and also Finland, increased contributions will include images channelled through specially vetted NGO's (for example, the National Center for Missing and Exploited Children in the US). Others still plan to develop software (for example New Zealand, the Netherlands, Germany, Moldova, Belgium and Slovenia) and forensic capabilities (UK) in order to facilitate the analysis and exchange of data in the ICSE database in the case of the former, and in order to detect new child sexual abuse images in the case of the latter. Further to this, the UK and US have launched a Task Force to Counter Online Child Exploitation with the aim of finding technological solutions, drawing on expertise provided by academia and the private sector (Report of the Global Alliance 2013, p.7–18).

In terms of investigative ability, whilst within the EU baseline legal requirements are set out in the EU Directive (European Parliament and Council 2011) on combating the sexual abuse and sexual exploitation of children and child pornography (see Chapter 5), within Europe

and globally there is a lack of coherence and consistency with regard to the substantive law that is in place across Alliance countries. Thus Switzerland, for example, is revising its criminal code to introduce new provisions on the definition of 'child' and the adoption of resolutions protecting children at UN level, whilst other countries are focusing on improving the procedural aspect of their legal framework (Slovenia, Georgia, Germany) through various means including legislation to facilitate international law enforcement and softer governance mechanisms for direct cooperation among law enforcement authorities.

Indeed the need for better coordination is highlighted as a key issue in the Report of the Global Alliance (2013, p.13), and the Ministerial Declaration on the progress of the Alliance issued in September 2014, identifies problems with 'processes and frameworks, both wholly domestic and multilateral in nature . . . [that] often fail to provide the expedient access to information and evidence that is necessary to effectively investigate and prosecute online child exploitation offenses' (Ministerial Declaration 2014). To this end, the US plans to create a new global platform with INTERPOL to enable and facilitate joint investigations, whilst, among other planned actions, certain countries seek to join the Global Virtual Task Force which seeks to build a partnership between law enforcement agencies, non-government organisations and industry to further enhance operational and strategic cooperation (Report of the Global Alliance 2013, p.14). There is also recognition that more needs to be done, beyond legal frameworks, in order to facilitate cooperation between public and private stakeholders, to strengthen dialogue and enhance trust relationships and operational cooperation. Finally, there is also the issue of improving cooperation with the private sector – through legislation (hands-on meta-governance) in order to strengthen the accountability of internet and peer-to-peer (P2P) service providers – and through Codes of Ethics and Conduct (hands-off meta governance) that require clear notice and take down procedures (Ibid., p.20).

The Global Alliance then, if a success story of EU–US joint activity in its first two years still has much work to do to eradicate the online exploitation of children. What the progress thus far highlights, however, is the need to achieve in partnership the necessary conditions for an effective security as resilience to emerge – in particular with regard to the legal and operational aspects of fighting the online sexual abuse of children. It is also clear that EU–US leadership will be essential in order for the Alliance to evolve further – and thus also imperative that the EU and US find ways to resolve their own legal, operational and strategic

differences more broadly when it comes to coordination, cooperation and collaboration on cybersecurity issues, if the Alliance is to prove a positive platform for best practice globally. Indeed EU–US leadership will be essential beyond the Alliance for the promotion of a common legal framework to fight cybercrime (currently the Budapest Convention) and cybersecurity standards within relevant international fora in order to ensure that the conditions for an effective security as resilience emerge.

Finally, the EU–US cyber dialogue was announced at the EU–US Summit in March 2014, with the aim of upgrading and broadening cooperation on cyber issues and to 'provide a platform to enhance exchanges between the EU and the US on cross-cutting cyber issues, key international developments and foreign policy related issues' (EU–US fact sheet 2014). The Information Society dialogue was also established so that the EU could engage in broader discussions on internet policy and governance, and information and communications technology. Whilst both these platforms provide further avenues for EU–US engagement on critical issues – they are likely to be useful only to the extent that they re-affirm joint commitments, agreed norms, and strategic goals – and ensure that momentum is not lost on critical issues of cybersecurity. Indeed, evidence from the inaugural meeting of the Cyber Dialogue confirms this, where both sides reiterated their commitment to: multistakeholder governance and an Internet that is 'inclusive, transparent, accountable and technically sound' (Press Release, 1st EU–US Cyber Dialogue); highlighted progress made in the EU–US Working Group; their commitment to human rights online; and global cyber capacity building. Given that these meetings will occur annually, they will certainly serve a strategic purpose – but the work of creating and building common understandings and responses will most certainly be done elsewhere – and in particular in the formal and informal arrangements that have been established at Working Group level and through more regular operational and tactical cooperation (for example, the FBI and EC3 on fighting botnets – see Chapters 4 and 5; or future cybersecurity exercises).

Conclusion: Converging on security as resilience?

This chapter has demonstrated that instances and patterns of divergence and difference as well as convergence and commonality exist between the EU and US across different issues relating to cybersecurity, including Internet governance, network and information security, and data privacy and protection. The connection between these dimensions,

and the complexity this creates, has implications for EU–US coordination, collaboration and cooperation on cybersecurity and importantly on convergence to an effective common security as resilience approach. More specifically, it makes it difficult to construct the necessary conditions for effective security as resilience if there are significant obstacles with regard to developing and enhancing a trusted partnership (for example, for how information is shared), and if cultures of cybersecurity differ to such a degree (national security Vs resilience approach) that common understandings of problems and therefore solutions cannot be agreed upon. Such problems are also exacerbated through a lack of coherence within the EU – as well as between the EU and the US – on specific issues and in particular in relation to the right balance between privacy and security in the pursuit of cyber criminals and the prevention of cyberattacks.

These obstacles and differences, of course, are not insurmountable. The EU and US are broadly convergent and committed to delivering an open, free and accessible internet through a multistakeholder model. This convergence has enabled the EU and US to form an effective partnership within international fora in order to pursue their vision of the Internet and IG. Although the Snowden revelations created tensions in this partnership, it also allowed the space for a more inclusive, accountable and multilateral narrative for IG to emerge and be projected, which the US had no choice but to engage with in order to placate the EU and other democratic states and IG stakeholders and to remain consistent with the values that the EU–US partnership projected for the Internet, its governance and its security. Demonstrating a willingness to multilateralise the control of the Internet must now be followed up in practice – bilaterally and more importantly in multilateral, multistakeholder fora – despite the tension this causes with regards to the national security first approach embedded within the US culture of cybersecurity. Indeed it is precisely because authoritarian states take such an approach to effectively create borders in cyberspace in the name of cybersecurity that the EU and US need to overcome any differences and pursue both a secure and open Internet for all.

There is a similarity in approach between the US and the EU in terms of the parameters and mechanisms for addressing issues of network and information security – and more precisely, protecting critical national information infrastructure. Indeed the US Cybersecurity Framework and the EU NIS Directive point to minimum cybersecurity standards, incentivising adoption of such standards and improving information sharing on cyber threats and attacks between the public and private

sector. In this sense, there is ample convergence and opportunity for the EU and US through organised cyber exercises, workshops, meetings and platforms (for example, a preliminary workshop was held to discuss this very issue in November 2014) to discuss creating common approaches and good practice in relation to critical infrastructure protection. However, the key difference between the two approaches taken – one voluntary (US) and the other regulatory (EU) might also undermine efforts to create 'commonality' and thus effective security as resilience in practice in relation to reporting, information exchange and information processing and possible real time responses. Importantly, the debate on mandatory Vs voluntary approaches is not yet resolved on either side of the Atlantic. Despite the EU regulatory approach and the US Framework – the efficacy of either one or other of the approaches have yet to garner sufficient support in Europe or the US; indeed there is disagreement among EU member states and between US public and private stakeholders on this. How the approaches will work in practice going forward – in conjunction with the reform of privacy and data protection rights – will provide a deeper understanding of how far a common approach can be constructed and what constitutes good practice given the legal and cultural contrast of the US and EU cyber milieus.

Data privacy and data protection have no doubt caused the most tension – and illuminated the greatest difference between the US and EU approaches to cybersecurity. Indeed, the Snowden revelations raised the issue of whether EU and US cultures of cybersecurity were compatible when it came to personal data collection and its use for intelligence purposes, given the logics that underpinned the approaches taken. The EU has taken a robust rights-based approach to reforming legislation on data protection for European citizens that has implications not just for cybersecurity but also issues relating to trade and use of social media across the transatlantic space. Whilst the US has also embarked on reform of the rights of its own citizens and those of non-Americans, as well as its legislation on data collection for intelligence, there are still unresolved issues, such as how mass data is collected, filtered and used, that impact on existing agreements such as the PNRA and TFTP. These issues need to be prioritised at the highest level of engagement – but also at operational and working levels, between the EU and US, if progress is going to be made in removing legal obstacles and rebuilding trust between the two partners, but also between citizens and governments in Europe and the US. This is important not just for constructing the necessary conditions for a security as resilience to emerge with regards to cyber issues, but also parallel issues such as the TTIP, given the intimate

link between the private sector, data collection by governments and intelligence agencies and the borderless nature of cyberspace.

If effective security as resilience is a real objective of transatlantic cooperation in cybersecurity and cybercrime, then the US and EU – not to mention certain EU member states – must, in the short term, have a serious conversation – and find a compromise – on the logics that underpin their respective approaches. Indeed the most insurmountable obstacle for EU–US convergence on constructing security as resilience going forward will be the vulnerabilities and insecurities created by a deterrence-based national security first logic. Whilst the EU logic emphasises resilience over offense and deterrence, certain EU member states prioritise the former (including the UK), creating inconsistencies in practice. Although this might well provide bilateral opportunities for individual EU member state collaboration with the US, more broadly, it undermines efforts to create a common approach between the EU and US based on agreed IG values and effective resilience. Moreover, it also makes less credible any joint EU and US efforts to project such values in relation to cybersecurity among non-democratic states that prioritise national security in order to protect their cyberspace.[12] Without such a compromise, convergence on a real and effective security as resilience between the transatlantic partners can only be achieved at the margins rather than in a comprehensive and transformative way.

8

Conclusions: Towards Effective Security as Resilience in the European Union?

Introduction

A central aim of this book was to analyse and provide a deeper understanding of the EU's evolving ecosystem for cybersecurity. Moreover, it sought to demonstrate how far the EU has travelled in constructing and embedding the conditions for an effective security as resilience to emerge in Europe, and beyond. Not only this, it has explored the relationship between modes of cybersecurity governance employed and types of resilience emerging, interrogating in particular the relationship and often tension between the hands-on approach and the hands-off and market based approaches to cybersecurity. In this context, the central pillars of the EU's Cyber Security Strategy (EUCSS) were assessed within a national and global context in order to address the central questions posed at the outset:

- How can we characterise and understand the EU's evolving ecosystem of cybersecurity governance?
- To what extent has the EU been able to construct a comprehensive and resilient approach to cybersecurity within the evolving ecosystem?
- What is the nature of the resilient ecosystem emerging in the EU?

What has been argued throughout is that utilising the notion of *security as resilience* rather than security of control, not only provides us with a sense of direction with regard to the EU approach in terms of the relationships it is constructing and constituting, but also a deeper

understanding of why and how the EU is travelling in such a direction, in terms of the actors and institutions involved and the global ecosystem within which they are operating. Moreover, it was suggested that problematizing resilience and adding nuance to how it is defined and understood conceptually, as well as taking a critical approach to security governance, allowed closer assessment of the shared logic(s) of resilient security governance emerging, and in turn, what this implies for the EU within the different spaces and levels that it must interact, in practice.

In this context, it was also suggested that an adaptable and flexible type of resilience should drive the EU's approach to cybersecurity and that the EU should focus on developing the conditions for effective cybersecurity resilience through appropriate governance mechanisms for it to become an influential actor in cyberspace and a leader with regards to good practice in cybersecurity and its many different dimensions. Note here that the purpose was not to be prescriptive about governance *per se*, but to trace the evolution of effective resilience and the governance mechanisms emerging that were chosen to achieve it across the different dimensions of cybersecurity assessed. Overall, a security as resilience approach built on and added to the existing conceptual literature focusing on cybersecurity more broadly and the sparse literature relating specifically to the EU (Klimburg and Tiirma-Klaar 2011; Dunn Cavelty 2013).

This final chapter will draw together the empirical and conceptual strands of the book and reflect on what the central findings imply for the EU's evolving cybersecurity strategy and policy. It will thus assess the implications of the EU approach taken with regards to cybercrime, Network and Information Security (NIS) and cyber defence, as well as for its role in member states and internationally – and in particular with regards to the future of the EU–US partnership. This is with the caveat and limitation that there are no concrete generalisable conclusions that can be made with regards to the resilience in EU member states overall. However, analysis of the data available (see Chapter 4) and a focus on the UK as a case study will allow at least some reflection on a leading member state and what can be learnt from good practices employed in the UK context. It will also outline lessons learnt more broadly, offer reflections on resilience and governance and provide recommendations on the future direction of strategy and policy for the EU if it is to move to more effective security as resilience in the future (Box 8.1).

Box 8.1 General conditions: Effective security as resilience

- Ability (including resource and mandate) and preparedness to adopt new basic operating assumptions and institutional structures
- Assumption of efficiency abandoned in favour of complexity in governance logics in order to avoid single points of threat and failure
- Coalitions of actors working together in 'partnership' to share information, construct new flexible and adaptive institutions and operating procedures, set the agenda and construct/implement policies
- Convergence amongst stakeholders on a 'common' logic(s), 'norms', laws and standards of security of resilience
- Evolution of a *culture of cybersecurity* at all levels among all stakeholders (awareness, education and so on)
- An integrated approach (coherence and consistency across layers, levels, actors)

The emerging ecosystem in the European Union: Security as resilience?

The EU's approach towards cybersecurity is, not surprisingly perhaps given that the strategy was not articulated until February 2013, formative in nature, with each priority area at different stages of development. In this context the cybercrime domain is most advanced, followed by the NIS domain and finally cyber defence, which has, comparatively speaking, only a very short history as a domain for development within the overall EU cybersecurity strategy. Whilst the strategy was constructed to create a coherent approach, it is still evident that there is much to be done between the responsible national, regional and international institutions, networks and agencies to realise this. Indeed, across the different dimensions of policy the EU must work to omit overlap in responsibilities and ensure effective working on issues of mutual interest. Moreover, there is much work to be done in securing both the resource and constructing the ecosystem to embed the necessary conditions for a security as resilience approach.

Within the cybercrime domain, although the legal aspect remains the most important in creating a clear framework for collaboration in information exchange, investigation and prosecution – whether through EU Directives and Regulations or ratification and implementation of the Budapest Convention – cultural and political obstacles have proven more difficult to transform within the different levels and layers necessary. Although there has been a step-change in governance terms towards a more hands-on meta-governance approach within the NIS domain, there is no clear consensus within the EU among stakeholders that this approach is the most effective with regards to building the necessary trust relationships necessary for effective partnerships to emerge. Whilst the European Commission selected such an approach in its evaluation of options for the NIS Directive, many leading 'cybersecurity' member states and business leaders are sceptical as to whether this approach will lead to the necessary trust for effective information sharing and provide the flexibility and adaptability required for the evolution of a deeper resilience among key stakeholders. For cyber defence, given the sensitivity around the issue for EU member states, the emphasis thus far has been on incentivising collaboration in the development of training, education and skills for the necessary audiences (military and civilian) – and thus on a meta-governance of coordination through formal but also informal channels of cooperation.

To what extent, then, can we conclude that progress has been made within the EU in facilitating the emergence of and constructing the conditions for security as resilience?

Cybercrime

Although cybercrime policy can be considered the most mature pillar within the EUCSS, substantive challenges exist to embedding the conditions for an effective security as resilience with regard to combating cybercrime in the EU. The many actors, processes, levels, layers and dimensions involved in creating an effective ecosystem make this a complex exercise and one that can only be achieved through incremental change given the importance and centrality of transforming cultures – ways of thinking and doing – in addressing the dynamic challenge of cybercrime. It is also clear that cybercrime does not sit in isolation from the challenges of cybersecurity more broadly. Beyond this, the Snowden revelations exacerbated the debate on privacy vs security, making even more complex the legal and cultural environment within which policy on cybercrime and cybercriminals could be pursued. Indeed, the PRISM affair has catalysed transformation in the EU legal dimension

as well as that in the US, with the predominant cultural shift, certainly in Europe, to ensuring individual rights are protected in EU law against mass surveillance in the name of security. The key implication in resilience terms is that of complex and clashing governance logics – and in particular reconciling the legal dimension with the operational and strategic dimensions of investigating and prosecuting cybercriminals.

Within the cybercrime dimension, obstacles remain but progress has certainly been made. Creating a culture of cybersecurity has been at the very centre of the EU's efforts of achieving security in the Information Society (IS) for many years, with a recognition that in order to address the causes and not just the symptoms of cybercrime, a multi-stakeholder, partnership approach would be required as well as a common understanding of the problem (definition) and the processes required. Within the 'drastically reducing cybercrime' priority in the EUCSS there is a focus on the legal dimension – national, regional and global – as well as the operational layer and coordination between and within all levels relating to cybercrime. These different elements speak directly to the conditions necessary – in the legal and operational layers primarily – for an effective security as resilience to emerge, and in particular to the criterion of creating a culture of cybersecurity within and between different dimensions of the emerging cybersecurity ecosystem.

In this context, platforms, legal conventions, working spaces, relationships and mechanisms have been developed for the purpose of fostering a convergent milieu for understanding and 'doing' cybercrime within and beyond Europe. For example, a majority of EU member states have signed and ratified the Budapest Convention which – although not immune to criticism – provides a platform for a culture of cybersecurity to emerge at the legal and operational level based on a common, if not completely harmonised, set of minimum standards, definitions and protocols. The limitations of the Budapest Convention within and beyond the EU of course need to be addressed in the medium term; with further scope and clarity being added to the rules and provisions in relation, for example, to the treatment and storage of seized information. More immediately though, and to at least ensure certain minimum legal norms for harmonisation – all EU member states should ratify and implement the convention – and seek to persuade states beyond the EU – through direct bilateral engagement and through relevant multilateral fora – of its efficacy in addressing cybercrime. In this context the Budapest Convention must be further supplemented by the EU's Directives and Regulations that relate directly and indirectly to addressing cybercrime in order to move beyond incentivising structures that

ensure minimum capacity building within and between EU member states (institutions, resource, skills and so on). Internationally, the EU must advance and make more prominent in its international cyber policy its efforts to facilitate capacity building within developing countries. It must also step up its efforts – not just at diplomatic but also working operational levels – to engage with those states that are reluctant to sign up to any conventions due to their 'national security' first approach to cybercrime and cybersecurity. Building understanding and trust within pockets of operational engagement at lower levels could certainly facilitate the removal of obstacles to collaboration and accelerate broader policy agreements in the medium to long term.

It is also important to recognise that new institutional structures as well as networks, platforms, alliances and strategies have evolved at the EU level to promote partnership, build trust and foster an integrated environment for addressing cybercrime. To this end, agencies such as EC3 and ENISA were created and mandated to tackle the issue of cybercrime in terms of respectively, addressing the operational and strategic aspects of cybercrime from investigation to prosecution and facilitating coordination among stakeholders within and between member states. The EUCSS (2013) has outlined a list of priorities in relation to cybercrime as well as other aspects of cybersecurity – and there has been a step-change in the legislation and governance of cybercrime that has sought to inject legal clarity into issues such as the definition of a cybercrime, data and information sharing, privacy, and investigation and prosecution. The EU's cybercrime initiatives have also seen the emergence of platforms such as the Safer Internet for Children and the European Strategy for a Better Internet for Children. Internationally, the Global Alliance against Child Sexual Abuse Online, has demonstrated what can be achieved when a coalition of actors work together to achieve specific objectives, even though much needs to be done to harmonise regulatory frameworks, to strengthen dialogue and to enhance trust relationships and operational cooperation among signatories.

In all of these developments the role of effective partnerships and trusted working relationships has proven to be important – the European Financial Coalition, a good example here. It is also clear that evidence and opinion points to the salience, in governance terms, of informal partnerships across and within countries for the fight against cybercrime to work effectively. Such arrangements, in particular when issue driven, provide the flexibility and incentives for key stakeholders – public and private – to work together in order to optimise resource

and expertise in combating cybercrime. However, whilst examples of good practice exist across the EU and globally of both formal (EC3, J-CAT), semi-formal (information sharing and analysis centres) and informal arrangements (issue-driven cooperation, for example, fight against botnets) between key actors (law enforcement, intelligence services, public bodies, private industry, CERTs and so on), much more needs to be done in relation to clarifying legal and procedural practices, enhancing operational resource, tools, capacity and training, creating synergies between different cultures of working across stakeholders, and embedding flexible governance mechanisms to ensure that an integrated system of working can emerge in the medium to long term. Here, evidence suggests that models of good practice need to be scaled up to work systematically across Europe and globally in order to provide a more overarching and sustainable structure for public-private cooperation. Creating a more integrated working environment with the requisite expertise – legal, technical, operational, strategic and policy – would certainly create procedural clarity and foster trust-based relationships through more regular interaction between key stakeholders in the fight against cybercrime.

Further to this, the asymmetry between member states and the resources (whether that is financial, legal, skills, expertise and so on) and institutions they have for combating cybercrime presents a major hindrance with regard to preparedness, harmonisation, mutual recognition and convergence. Relationships between different stakeholders and agencies are formative and evolving – within and between countries – so whilst there is some convergence around the awareness of what is required – in practice there are still substantive barriers to achieving effective collaboration, coordination and cooperation. Moreover, whilst the EU has many initiatives to tackle cybercrime, what is still required going forward is a sense of how they join together and indeed what sort of impact they are having with regard to operational, legal and regulatory, technical, training and cultural aspects. What we can safely conclude on the basis of the evidence presented in this book, is that the conditions for security as resilience in cybercrime in the EU are formative but progressive – although not yet integrated to the degree that is required to combat cybercrime effectively. For this to emerge in the medium to long term, barriers must continue to be broken down between relevant stakeholder communities – and sustainable working relationships and partnerships based on a common terminology constructed. Only in this way can the EU ensure that the ecosystem being constructed to address the challenges of cybercrime will allow Europe

to protect its systems and networks against cybercriminals and ensure a secure platform for economic growth in the digital economy.

Network and information security

The EU's approach to NIS has gradually evolved, in governance terms, from a hands-off meta governance, voluntary approach to information sharing and reporting of major incidents, supported by numerous platforms such as the EP3R and the EFMS, and ENISA as a key facilitator of collaboration and capacity building, to a hands-on mandatory approach proposed by the NIS Directive (2013), which as noted in Chapter 6, has been greeted with a mixed response in deliberations within the EU institutional milieu to agree a final form.

Throughout this journey, lessons were learnt on how to incentivise public-private collaborative and platforms to facilitate this – key being that of ensuring that any such platforms should offer clear goals around defined issues, and that any work should have a clear outcome with regards to how it would feed into the EU's evolving cybersecurity legislative and research agenda. The EP3R, in this sense, evolved into and was subsumed under the NISP, which whilst proving to be a more effective platform in terms of producing clear deliverables that will feed in to the achievement of EUCSS and H2020 research objectives, still raises questions of sustainability for European-wide public-private collaboration. The EU, thus, needs to think clearly about how such a platform can be taken forward in the medium to long term to build and maintain the necessary inclusivity, trust and regular interaction needed for effective public-private cooperation, coordination and collaboration.

With regard to the EFMS, it has clearly been able to produce key EU documents (European Principles and Guidelines for Internet Resilience and Stability), but unless it is taken more seriously by member states, it will remain a symbolic rather than an effective platform for information sharing and exchange of good practice. More regular and informal meetings around critical issues at different working levels might prove more useful in the medium term in order to build the trust necessary for fruitful interaction. It may also be the case that the NIS Directive, when finalised and agreed, will provide a concrete issue on which officials can focus on with regards to the practice of implementation and its implications. Key lessons were also learnt from conducting cybersecurity exercises within Europe and between the EU and the US, with the most valuable being that as a platform for enhancing learning on the technical, political (institutional), operational and strategic levels, it was effective, and should continue to be utilised as a key tool for enhancing

knowledge, understanding and trust among key stakeholders. Indeed, resource should be enhanced to increase the frequency of such exercises not just on a macro level (Europe wide/international), but also on a micro level (between specific public and private actors), in order to increase stakeholder interaction, awareness of different working cultures, and the skills and capacities needed to ensure that effective institutions, partnerships and common working practices can be established. That is, to ensure that a culture of resilience is embedded throughout the European ecosystem thus creating a virtuous circle of learning from doing at different levels and across borders.

The proposed NIS Directive – the centrepiece legislation that accompanied the EUCSS – on the one hand, has achieved general consensus on the need for establishing minimum capacities and capabilities across all EU member states (for example, a national CERT) in order to construct cybersecurity resilience, given the differentiation and asymmetry that exists. On the other hand, the scepticism that has surrounded its all-inclusive critical infrastructure sector approach, has led to a watering down of the Directive by the European Parliament and EU member states in terms of its original scope, which potentially has consequences for its effective implementation and practice – and importantly for constructing the conditions for security as resilience through trustworthy partnerships and coalitions of actors adopting a common 'approach' to reporting and effective information exchange. A compromise will thus have to be found in the final phase of deliberation of the NIS Directive in the Council of Ministers, which ensures a balance between formal mandatory reporting and informal, trust-based exchange of information. Only in this way can an embedded culture of cybersecurity emerge over time, and a move to an audit, tick-box culture be averted within Europe that creates further barriers to effective stakeholder integration and collaboration.

Much like cybercrime then, and very much related to it, the NIS ecosystem is evolving, although far from optimal in embedding the necessary conditions for the diffusion and implementation of an effective security as resilience approach across Europe, or indeed through its key international partnerships. This can only happen in the short term if there is sufficient 'common' ground between all stakeholders on the most effective mode(s) of governance for incentivising effective working relationships with regard to information exchange, sharing and processing, and in the medium to long term, if both formal and informal channels and platforms create sustainable, trust-based relationships that allow good practice to flourish and a genuine culture of

cybersecurity to emerge. The European Commission, at this moment in time, believes the proposed NIS Directive will provide the platform for this to happen, or at least the minimal platform for a European upgrade; in practice, however, this will very much depend on how far a compromise can be found on its final form (and implementation) between national and indeed professional cultures of cybersecurity within and between countries of the EU.

Cyber defence

Cyber defence is the newest and therefore least developed strand of the EUCSS; and it is important to acknowledge that the EU's conception of cyber defence is grounded in a security as resilience logic – to self-protect and ensure access to military and linked civilian assets that are utilised for military purposes (a soft power approach). This sits in direct opposition to the US, for instance, that operates within the logic of cyber offence and enhancing cyber weapons in order to adequately equip itself for fighting the cyber enemy (a hard power approach). This is mainly because the EU does not have its own military assets *per se*; but certain EU member states, of course, do, and invest in cyber weapons, whilst others that do not have cyber weapons include a military perspective in relation to cyber defence within their national cybersecurity strategies. Others still, have not defined a cybersecurity strategy and do not fully understand or engage with cyber defence issues, even though they are familiar with them.

This diversity and asymmetry in knowledge and preparedness, is more marked in cyber defence than the other strands discussed, with particular problems identified across member states in developing cyber defence doctrines, appropriate organisation and training, and the facilities necessary for cyber defence. More positive, was that in the areas of leadership, personnel, and interoperability, there was a much higher level of development. It seems that member states with a high level of maturity in their thinking amongst key decision makers about cybersecurity are also more advanced in relation to cyber defence capability.

At EU level, threat analysis and intelligence gathering capability is emergent and incident response needs to be deepened within the complex organisational set-up at operational level. In addition to this, knowledge and understanding of military specific standards and tools needs to be drastically improved and the culture of good cybersecurity practice needs to be nurtured in order to make it more effective. Having said this, under the leadership of the EDA, primarily, initiatives

have developed at pace, in seeking to meet the objectives of the Cyber Defence Policy Framework. Strands such as training and education are more highly evolved than others at European level, with ad hoc projects operationalised by the EDA to enhance knowledge and capability proving to be useful platforms.

However, many challenges still remain in terms of enhancing resilience within the cyber defence strand, both at EU level and across EU member states. First and foremost is that not all EU member states cooperate on cyber defence; this is underpinned by a CSDP mandate with no obligation for states to engage. However, this makes it more difficult for collaboration and thus shared understandings and approaches to emerge at EU level, in what is quite clearly an area of shared interest and threat for all EU member states. Second, issues also arise within the EU and between the EU and member states in relation to the synergies and thus approaches to be taken in protecting military operations that often rely on private critical infrastructure. Clear definitions, doctrines, processes and procedures need to be developed in order to ensure clarity in approach and assessment of cybersecurity threats within different phases of any mission. In addition, training must be further enhanced through increased interaction between personnel in established military CERTs and civilian government or national CERTs in order to improve understanding of shared risks and the practices and processes required to address cyber threats in cyber defence.

Whilst the EDA is certainly proactive in developing such interaction through various training platforms, this needs to be scaled up in the short to medium term in order to enhance the understanding among national and European actors and agencies on what is required in order for resilience to evolve in cyber defence. Related to this, is training and retaining cyber specialists for the military; the EU, in conjunction with member states, must first, enhance targeted cyber military training in the short term and second, develop policies and incentives for retention in the medium to long term, in order to ensure that the requisite skills and knowledge are available to sustain resilience in cyber defence.

Finally, whilst potential exists for the evolution of more effective international partnerships to address cyber defence issues, here too, progress is constrained by complexity in the formal process – in particular in relation to NATO – even though obvious synergies exist. Here the EU must continue to explore formal solutions and perhaps as important, exploit further informal relationships that have evolved between cybersecurity officials of the EU and NATO at different working levels.

Reflections on the domestic and international

As alluded to throughout the chapters of the book, cybersecurity incorporates many layers and levels that do not sit in isolation from each other when discussing the evolution of security as resilience. To this end, when analysing EU progress it has been important to understand the domestic and global context in which the EU must act and influence. Whilst EU member state preparedness overall was not addressed in detail in this book beyond the UK, certain general implications can be discerned from the evidence that has been presented across the three pillars. Moreover, the UK experience has provided a detailed idea of practices in cybersecurity that might be transferred to other domestic arenas and European agencies and fora; whilst also at the same time highlighting that even in advanced member states different logics and approaches can create potential barriers to developing a European and global security as resilience approach.

In general, it is clear that there are different levels of maturity among EU member states across the pillars of cybersecurity – cybercrime, NIS and cyber defence. Progress has been slow, but forthcoming – one key indicator is that of the evolution of cybersecurity strategies across 18 EU member states. It is also equally clear, however, that the dominant trend that is likely to remain in the short to medium term is of asymmetry across the European space – that is, EU member states and the EEA countries (Iceland, Lichtenstein and Norway). Here there are different levels of development – evolving cultures of cybersecurity across different layers – but ultimately we are still quite far from optimal security as resilience whether in relation to procedures for information exchange and cooperation, institutions and processes for security incident management and reporting, network adaptability, legal frameworks for ensuring a balance between privacy and security, or awareness raising. What can be concluded tentatively is that there is awareness among all EU member states and a common understanding of what constitutes – in terms of minimum requirements – a resilient ecosystem. However, significant barriers exist within and across member states for achieving this in practice – cultural, institutional, resource, legal – and in certain cases, an underdeveloped understanding and awareness of the potential cyber threat.

The case study of the UK, considered a leader in cybersecurity policy and thinking within the EU, has advanced its cybersecurity ecosystem substantively through a holistic approach in the last four years. The UK government's approach underpinned by a voluntary market-based

and hands-off logic, however, sits in direct contradiction to the mandatory approach taken within the proposed NIS Directive. In this the UK is not alone in insisting that a voluntary approach is most likely to lead to sustainable and trust-based information sharing between key stakeholders – indeed the split in the Council of Ministers seems to be between advanced member states that advocate this position and less advanced member states that support a mandatory approach. The UK certainly provides good examples of how such an approach can work – through initiatives such as CISP – but such initiatives are not unproblematic. Importantly for the development of a security as resilience across the EU space, is the potential inconsistency in practice that may occur if an effective compromise on the NIS Directive cannot be found that can accommodate voluntary and mandatory logics. A convergent position needs to be found that ensures a culture of information sharing can emerge that moves beyond procedural reporting of incidents to demonstrate compliance to one of effective and timely information exchange based on the mutual interest of addressing cyber threats. The UK must also recognise that in the medium to long term non-participation in the EU's cyber defence efforts is detrimental to its own interests; developing capability across Europe can only enhance resilience in the UK, in particular given the interconnection between the civilian and military architecture and assets in the context of EU missions.

On good practice, there are certainly lessons that can be learnt and transferred with regard to partnerships – formal and informal – in education, awareness and in particular on the operational side of cybercrime. In this sense the J-CAT initiated by the UK National Crime Agency and semi-formalised within the EC3 is a demonstration of how partnerships consisting of multiple stakeholders can work effectively to, for example, take down botnets or child pornography networks. Such ad hoc governance also provides valuable insight into the obstacles for doing this across borders – including legal and procedural in terms of access to IP addresses, or indeed access and use of information in real time. In addition, it facilitates the construction of innovative mechanisms – such as encryption systems that will address issues of privacy whilst also ensuring that information shared is specific to a particular task or case investigation rather than exchanging bulk data. Whilst such mechanisms are formative at best, they should be supported and resourced further by the EU as they clearly offer not only an effective way of protecting against cybercrime, but unearth problems and find solutions on how to achieve effective responses to attacks and threats.

Within the global cyber milieu, there is much contestation as well as consensus on how to govern the different dimensions of cybersecurity. As indicated in Chapters 3 and 7 there is a clear recognition in the international community that global norms to govern the behaviour of states and other actors are required if a global culture of security is going to emerge in cyberspace, and there are also guidelines and a broad consensus on some of the key principles that should underpin any global framework. However, whilst there is a certain convergence at the level of broad principles and norms, consensus is not evident in the interpretation of what such norms imply for Internet governance and in turn cybersecurity across different state borders. Indeed several tensions are prevalent that restrict the construction of optimal conditions for security as resilience to emerge. Prominent among these are: the tension between the commercial logic and the security as resilience logic; the sovereign national security logic of certain states and the open, multi-stakeholder approach advocated by many leading 'Western' states and international organisations; and finally, and very much connected to the latter, the tension between privacy and security, and the debate on how a balance can be achieved to ensure that the rights of individuals are protected in the collection of data for securing cyberspace.

However, this is not simply a case of the 'West' vs the 'Rest' – contestation is apparent in different spaces, and is constantly shifting between varying coalitions of actors. Thus whilst the EU and US certainly agree on the need for an open, accessible and resilient Internet and a multi-stakeholder model for Internet governance in contrast to states such as China and Russia that promote a state-driven, intergovernmental system, there are clearly also disagreements which materialise from the security logics that underpin their approaches to cybersecurity. The Snowden revelations, in this sense, served to exacerbate the differences and reduce the trust between the EU and US, on issues related to privacy vs security, and cybersecurity more broadly. They also, importantly, provided a justification to authoritarian states for their national security approach, underpinned by 'bordering' the Internet in order to make it secure within their cyberspace.

Whilst the Snowden revelations caused a certain degree of tension between the EU and US – they also triggered a period of reflection, deliberation and reform on both sides of the Atlantic. This has served to rebuild some trust even though it has not necessarily meant a convergence in approaches, or indeed practice across the different dimensions of cybersecurity. For the EU and US fundamental differences still exist within the legal and cultural realm – but practical compromises in

practice are not beyond the realms of possibility and are indeed necessary, if both the EU and US are to forge effective common working processes and mechanisms for addressing cybersecurity, and if they are to credibly defend and diffuse the core values of Internet governance that they project in the international arena. The current contradiction between values espoused and actions taken, in particular by the intelligence services on either side of the Atlantic (for example, the NSA and GCHQ) must be addressed if an effective security as resilience is to be achieved in the EU–US partnership; if not, it has implications not just for existing agreements on PNR and TFTP, but also broader issues such as negotiations on the TTIP. It also has implications on the influence that the EU and the US can wield in the international arena for cybersecurity. The tensions and contradictions at the centre of the different logics within the (geo)politics of cyberspace – represented within the (not necessarily convergent or common) plethora of codes of conduct, guidelines, principles and international laws and charters, are what the EU must continue to engage with, draw from and proactively influence and shape, if its own efforts to create a comprehensive and resilient ecosystem of resilient security governance are to bear fruit. For this to occur, however, it is important for the EU to continue with its conference diplomacy, bilateral activities with strategic states, and activities within international organisations such as the OECD where it has played a key role in producing cybersecurity Confidence Building Measures (CBMs). It is also important, however, to think more innovatively about more regular multi-level, functional interaction and engagement (research, operational work) and the resource that is required to do this.

Reflections and final thoughts

This book has provided a broad pointer in terms of the direction in which the EU is travelling with regards to achieving what was described in Chapter 2 as socio-ecological or Type 3 resilience in its cybersecurity policy and strategy. Using the general conditions constructed from the literature for the achievement of effective security as resilience, and exploring dominant governance modes utilised by the EU within its evolving ecosystem has provided a sense of where each EU cybersecurity pillar analysed sits with regards to progress internally and within the international context. Of course, as comprehensive as the analysis of these pillars has been, as iterated from the outset, there are many micro and macro aspects that could not and have not been covered that would have to be interrogated in research going forward to give a more holistic

sense of where the EU is across the different dimensions of its strategy, the issues and priorities that it seeks to address, and the actors and spaces that it engages with and in. In this context, fruitful research agendas moving forward would involve a more substantive, qualitative investigation of the development of the conditions for security as resilience across the 28 EU member states; and the obstacles to collaboration on cybersecurity and cybercrime issues between key stakeholders and agencies in and across EU countries and between the EU and international partners and countries.

The limitations above aside, the analysis raises questions of the utility of resilience as a guiding concept for cybersecurity strategy, and the security as resilience approach for understanding what is and should be emerging from the EU's efforts. There are three interrelated aspects to this: practical, theoretical and normative. On the practical level, first and foremost, although it is possible to point to general trends and patterns of resilience, it is difficult to measure and assess conditions for resilience directly or indeed accurately – in particular in terms of cultural transformation in practice. Where such programmes do exist (for example, in the US) difficulties still remain with regards to the indicators chosen, the stakeholders consulted and the adequacy of the data added (Cavelty and Prior 2013, p.3). Such general problems with measuring resilience in security contexts are compounded even further in the field of cybersecurity given the multitude of layers, levels, spaces and dimensions that need to be measured. However, if the concept of resilience *in* cybersecurity is to avoid the accusation of ambiguity and vagueness targeted at human security over the years, then parameters for how to achieve resilience in a practical sense, in particular in the EU and European space, would have to be more specifically designed for purpose beyond general conditions, to concrete objectives and actions in priority areas (and micro elements within these). Here, valuable lessons might be learnt from evolving guidelines for achieving integrated security resilience in parallel areas of concern (for example, crises and disaster management; see Comfort et al. 2010; Chmutina et al. 2014).

This is not to say that security as resilience should be accepted uncritically as a panacea for effective cybersecurity. The analysis of the EU's cybersecurity ecosystem has demonstrated that varied perceptions and logics of resilience exist at different working levels – and that the task of reconciling cultures of cybersecurity towards a common understanding and way of thinking and doing, is challenging. Understanding how such perceptions and the construction and performance of resilience

play out and evolve in practice – political, economic, legal, operational and strategic – will therefore be critical to enhancing our knowledge on the impact it has, and indeed on the evolution of the concept in the EU context as a strategic narrative that can guide cybersecurity. Future research, then, should delve deeper into how resilience is performed in cybersecurity contexts – where it is contested and challenged – and the material and non-material (cultural) effects it has on creating more rather than less security in cyberspace.

Finally, in relation to the normative dimension, the implicit argument throughout the analysis of the EU's emerging ecosystem for cybersecurity has centred on a particular type or notion of security as resilience, underpinned by concern not for national security of the state but security of the individual in cyberspace. The analysis has suggested, in the case of the US as well as countries within the Shanghai Cooperation Organisation (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan) and the EU (such as the UK), that a national security approach that prioritises protecting cyberspace through perpetuating cyber warfare and prioritising mass surveillance and espionage, can only lead to negative effects on both the freedom of the Internet and its security. Indeed as articulated so well by Dunn Cavelty (2014), a national or traditional security approach to cyberspace can only lead to a cybersecurity dilemma and further vulnerability, not resilience.

The EU approach thus far, as defined in its cybersecurity strategy and in its practice, is underpinned predominantly by a security as resilience logic; that of self-protection through development and projection of soft power (protective defence) and not hard power (offence) (see Chapter 2). However, despite the EU's general orientation, the management of risks related to information and data assurance processes is also visible in its policies and platforms, and that of its member states. Traditional risk methodologies (found in Type 2 resilience – see Chapter 2), despite their widespread use in cybersecurity it has been argued by certain commentators, are incompatible with a security as resilience approach (socio-ecological). Such methodologies fit with the engineering definition of resilience that assume linearity and predictability, but are fundamentally flawed in the context of complex networks and risks where uncertainty mitigates any accurate prediction of events (Dunn Cavelty 2013). This said, the EU through initiatives such as the NISP, and its attempts to incentivise and create sustainable partnerships and working systems for information sharing and reporting, as well as operational aspects of cybercrime, have demonstrated that the EU is framing and constructing its actions within a security as resilience logic. In this sense

the EU cyber resilience ecosystem is formative but also variable across its dimensions. The challenge, in order for the EU to secure cyberspace and protect the Internet governance values that it espouses and projects, is to ensure that resilience, not traditional approaches to national security and risk, are sustained and developed front and centre of its policy evolution, and that the concept is firmly embedded, clearly elaborated and effectively implemented in its cybersecurity practices. Effective security as resilience in this way will evolve through a process of iterative learning and reflection in specific arenas, avoiding the generality that could render the concept redundant.

Finally, certain reflection is required on the meta-governance of cybersecurity within the EU and its relationship to constructing a security as resilience approach in the European space and international context. What is emerging in the EU is hybrid governance across and within the main priority areas of its cybersecurity strategy; that is a mix of hands-on, hand-off and meta-governance of identities approaches. What has become apparent throughout the analysis of the EU evolving system of governance for cybersecurity, however, is the move towards a hands-on approach to establish the necessary conditions for security as resilience – whether this is in the form of mandatory reporting in the NIS Directive or increased regulatory and legal clarity in the field of cybercrime. This is even though such an approach is contested (that is, mandatory reporting) – within the EU and between public and private stakeholders in the European and international contest, as alluded to above.

There is thus no clear picture of what the optimal approach for achieving resilience with the EU ecosystem is – but rather a dynamic debate on how trust-based relationships conducive to sustainable, collaborative platforms are best conceived. This said, a key lesson that might be derived from the research and indeed the practice within Europe is the critical role of multi-stakeholder, informal, ad hoc governance arrangements at the operational working levels, that allow targeted action on specific issues, as well as more semi-formal and formal arrangements that allow regular interaction between relevant stakeholders (for example, cybersecurity exercises, staff secondments). Such emergent arrangements subsequently serve to increase knowledge and understanding between relevant actors, creating spaces where different cultures of practice can be accommodated to create the necessary conditions for a security as resilience to develop. To this end – and compatible with the adaptability and flexibility required in a resilient EU cybersecurity system – space and support for experimental, hybrid forms

of governance should be resourced and encouraged, in conjunction with more sustainable public-private platforms; in particular where evidence suggests that this might well be the most innovative way in which trust-based relationships can be built and solutions to cybersecurity challenges in the EU and Europe can be found.

Notes

2 Conceptualising Security as Resilience in Cyberspace

1. Sliwinski focuses his analysis on the EU as a cybersecurity agent, but whilst invoking the notion of cyber power, it is not defined or problematized in any detailed way; indeed it is simply suggested that the EU, to be effective, must develop different forms of cyber power (compulsory, institutional, structural and productive). This, however, is to ignore the specific nature of the EU as an actor and an agent in cybersecurity (that is, it is not a conventional state). See also Christou (2014) and Miriam Dunn Cavelty (2014) who suggest that the EU should focus on building its 'soft power' based on its values and a resilience approach.
2. Although see Dunn Cavelty (2008b) where the move from governance to meta-governance is proposed in the context of the Swiss case (Critical Information Infrastructure Protection).
3. See Dunn Cavelty (2009) for a more nuanced analysis of the securitization of cyberspace in the US.
4. Although the relationship between security and resilience has been analysed more extensively in the literature. See Dunn Cavelty and Prior (2013); Coaffee and Fussey (2015).
5. Even though it does not claim to go as far as Brassett and Vaughan-Williams (2015) who put forth the concept of 'performative ecologies' in order to emphasise the fluidity and contestability of resilient discourse, as well as to highlight its non-material effects.
6. Defined as an 'indirect form of top-down governance that is exercised by influencing processes of self-governance through various modes of coordination' (Shore et al. 2011, p.6).
7. Dunn Cavelty's work (2013) is an exception, and intuitively germane to the argument in this book. She unpacks both resilience and cyber power in order to analyse the EU's emergent cybersecurity system. However, this is in the form of a short working paper and does not provide a comprehensive analysis of the EU cybersecurity strategy and EU policies and initiatives.

3 Cybersecurity in the Global Ecosystem

1. Note that this chapter cannot cover all organisations and thus excludes many informal initiatives/networks (for example, the Internet Engineering Task Force, Institute for Electrical and Electronics Engineers, Electronic Frontiers Foundation, Forum of Incident Response and Security Teams, The Meridian Process, London Action Plan, European Government CERTs group, and so on) and formal bodies that are active in cybersecurity. For an overview of the role of these organisations see European Parliament (2011)

and ITU Report (2011). See also the IMPACT website: www.impact-alliance.org. For the global south and Asia also see Kshetri (2013) and Deibert et al (2012).

2. The technical standards which were developed by the Internet Engineering Task Force (IETF).
3. In addition, and important in the context of resilience, DNSSEC does not directly address the problem of maintaining the availability of domain names (see Sommer and Brown 2011, p.59–60).
4. For a list of registrars that support DNSSEC see: https://www.icann.org/resources/pages/deployment-2012-02-25-en.
5. See Malcolm (2008) for a comprehensive overview and critical analysis of the IGF.
6. The Framework Directive for Electronic Communications (2009) already imposed reporting obligations on electronic communications providers for telecoms providers and data controllers, but the NIS Directive represented a clear step-change with regard to the governance rationale for *all* owners of critical infrastructure.
7. This subgroup established the 24/7 network, in order to facilitate the investigation of terrorist and other criminal cases involving electronic evidence between countries. It provides high-tech expert contact points in participating countries (approx. 45) which facilitate information sharing against cybercriminals (see http://www.oas.org/juridico/english/cyb20_network_en.pdf).
8. See www.impact-alliance.org.
9. The ITU also published a report on understanding cybercrime in September 2012, 'Understanding Cybercrime: Phenomena, Challenges and Legal Response'. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.
10. The NCIRC Coordination Centre is the first tier of NCIRC and is responsible for coordination of cyber defence activities within NATO and between NATO and international organisations (that is, EU, UN/ITU, OSCE, etc).
11. The OECD first produced Guidelines for the Security of Information Systems in 1992. In addition to these and the revised guidelines produced in 2002, the OECD has developed complementary recommendations concerning guidelines related to information society, including privacy (1980) and cryptography (1997).
12. Those that had not ratified it at the time of writing (March 2015) include: Greece, Ireland, Luxembourg and Poland. Sweden ratified it in 2014.
13. See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.
14. See Weber (2014) for an analysis of the convention and its application in the USA.
15. See Council of Europe: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp.
16. Although, see speech by the Head of Anti-Terrorism Issues for the OSCE for an exploration of policy options for addressing cybersecurity issues (Perl 2010).
17. OSCE Conference on 'A Comprehensive Approach to Cyber Security: Exploring the Future of the OSCE Role', Vienna, Hofburg, May 2011.

4 National Cybersecurity Approaches in the European Union: The Case of the UK

1. This is according to ENISA. See http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world. It must be added though that this does not mean the countries listed do not necessarily have a strategy – Cyprus, for instance does, but it is not on the ENISA website as it has yet to be translated to English.
2. Other potential sources of information on national country preparedness, such as the ITU's cybersecurity index does not, at the time of writing, provide any results for Europe. See http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.
3. As identified by ENISA and indeed a House of Lords EU Committee Report (2010, para 24).
4. The first version of which was published in 2009: 'Strategy of the UK: Safety, Security and Resilience in cyberspace'. It should also be noted here that the UK government had also developed National Information Security Strategies (2003, 2007) prior to this which outlined the initial steps and measures for assuring the integrity, availability and confidentiality of Information and Communications Technology systems and the information they handle.
5. For more on cybercrime strategy, see Cyber Crime Strategy (2010).
6. Baroness Pauline Neville-Jones is former Minister of State for Security and Counter-Terrorism (2010–2011). She has also acted as the government's Special Representative to Business on Cyber Security.
7. Note the Chatham House report produced by Cornish et al. (2011) focused on CNI and cybersecurity, and not all dimensions of cybersecurity.
8. The Office of Cyber Security and Information Assurance (OCSIA) manages and coordinates the programme with the Minister for the Cabinet Office providing oversight (The UK CSS: Landscape Review 2013, p.11).
9. With additional resource being freed up by merging the existing Computer Crime Unit within MPS into the PCeU.
10. Nick Hopkinson was formerly head of GCHQ and CESG.
11. This is done by disrupting the infrastructure enabling criminals to use the malware to raid bank accounts. More specifically, it entails seizing computer servers which form the command and control system for the Trojan, and taking control of the domains Shylock uses for communication between infected computers.
12. It must be pointed out here that instant access is not always assured even when investigations are police led. This very much depends on the relevant law in each country.
13. Reflected in its budget spend with the largest portion going to developing national sovereign capability to detect and defeat high-end threats (£253.8m in the first three years and £93.2m in year four). For detailed breakdown see 'Update on the National Cyber Security Programme' (2014, p.7–8).
14. Chris Gibson is the Director of CERT-UK.
15. See also Herrington and Aldrich (2012, p.301) on the GCHQ paradox with regards to secrecy and information sharing. The December 2014 update report from the Cabinet Office indicates that such mechanisms are being

expanded with GCHQ aiming to 'share timely and usable intelligence on hostile state and cybercrime activity with security-cleared personnel in Communication Service Providers (CSPs)' (2014, p.13). How far this resolves the broader issue of sharing in real time with all relevant stakeholders, however, is not clear.

16. See Cyber Essentials Scheme (2014). Requirements can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf.
17. To enable companies which supply cybersecurity products and services to the UK Government to reference this publicly and give added credibility when pursuing business (for example, overseas).
18. See in relation to this the Trustworthy Software Initiative: http://www.uk-tsi.org/.
19. See: http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map.
20. Even though how this is interpreted in practice might very well render it irrelevant.

5 The European Union and Cybercrime

1. Defined here as the 'broad range of different criminal activities where computers and information systems are involved either as a primary tool or a primary target' (EU cybersecurity strategy 2013, p.3). Cybercrime includes attacks against information systems, content related offences such as the incitement of racial hatred and traditional offences such as fraud and identity theft.
2. Botnets are networks of compromised computers infected by malicious software that can be remotely activated to perform specific actions, including cyber-attacks (such as denial of service attacks or spamming).
3. The caveat here is that at the time of writing many of these measures are still under discussion within the EU decision making structure (or indeed under construction), so a full assessment of all Directives/proposed actions is not possible.
4. To facilitate the implementation of this the European Electronic Signature Standardisation Initiative was also launched.
5. Of course, legal measures already existed across different policy sectors for the protection of privacy, data protection, telecommunications data protection and service security (art.4 and art.5), with the EU framework for telecommunications services outlining several provisions for 'security of network provisions' and 'network integrity' (restated in the Regulatory Framework for Electronic Communications Services in 2002).
6. With a commitment to introducing legislation by 2007.
7. Which was elaborated on more specifically in its communication 'Towards a general policy on the fight against cyber crime' (European Commission 2007).
8. The European Security Research Innovation Forum was set up and reported in 2009 on how the public-private relationship could be taken forward with regard to European security in general (and including cybersecurity

and crime). See: European Security Research Innovation Forum (ESRIF) Final Report (2009).

9. This built on the 1995 Data Protection Directive (European Parliament and Council 95/46/EC) and the 2002 Directive on Privacy and Electronic Communications (European Parliament and Council 2002/58/EC) (amended by the Directive 2009/136/EC).
10. See, for example, http://www.edri.org/files/dr_letter_260911.pdf.
11. See, however, Porcedda (2012) on proposals for reconciling privacy/data protection and security through a technical rather than national security approach.
12. See Drewer and Ellermann (2012).
13. Replacing Directive 95/46/EC (European Parliament and Council 1995).
14. Replacing Framework Decision 2008/977/JHA (Council of the European Union 2008).
15. Still under negotiation and discussion in the Council of Ministers at the time of writing (March 2015) – see Chapter 7.
16. Porcedda (2012, p.63–64) also discusses this in the context of the problems that arise with regard to cloud computing.
17. Framework Decision 2004/68/JHA on combating the sexual abuse, sexual exploitation of children and child pornography (Council of the European Union 2004) and more generally before this outlining the rights of victims of crime, Framework Decision 2001/220/JHA on the standing of victims in criminal proceedings (Council of the European Union 2001). The latter was also updated and replaced by a Directive: 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime (European Parliament and the Council 2012).
18. The Safer Internet Programme was launched in 1999. See: http://ec.europa.eu/information_society/activities/sip/policy/index_en.htm.
19. The EFC aims to combat the production, distribution and sale of child pornography images on the Internet. See: http://www.europeanfinancialcoalition.eu/document.php.
20. Although some countries are more progressive than others (see Chapter 4). There are also initiatives that have been launched at European level such as European Cyber Crime Month – supported by ENISA and DG Connect – that takes place in October each year an aim of which is to promote cybersecurity awareness and training among citizens.
21. Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February on attacks against information systems – COM(2008)448 (European Commission 2008).
22. Council Framework Decision 2005/222/JHA (Council of the European Union 2005).
23. This with the caveat that the strategy was only published in February 2013, with its main accompanying Directive on Network and Information Security still making its way through the EU decision-making process at the time of writing (March 2015).
24. Indeed, the EU's Framework Decision on Attacks against Information Systems (2005/222/JHA) incorporated some of the convention's central concepts and definitions in order to bring this into EU law and define minimum sanctions for defined cybercrime offences (Council of the European Union 2005).

25. Those that had not ratified it at the time of writing (March 2015) include: Greece, Ireland, Luxembourg and Poland. Sweden ratified it in 2014.
26. Cooperation has also been promoted through schemes such as the European Government CERT (http://www.egc.org), and initiatives such as the TERENA TF-CSIRST (http://www.terena.org/tf-csirt) and FIRST (http://www.first.org).
27. The ENISA report concentrated on National or Government CERTs, that is, CERTs acting as a national Point of Contact (PoC) for collaboration and information sharing with other national CERTs in the EU or CERTs responsible for the protection of governmental and public administration networks (ENISA, Flair for Sharing 2011, p.20).
28. For example, national cybersecurity centres, other CERTs (domestic, EU and non-EU), intelligence agencies, non-European LEAs, the private sector, and any relevant international entities (such as, the International Criminal Police Organization (INTERPOL)).
29. ENISA reported (ENISA, Give and Take 2012, p.41) that at least two countries described cases where CERT action led to them becoming liable through data protection laws. This point is salient in relation to the different types of CERT that exist not all with a clear mandate based in primary legislation for sharing and processing data.
30. Not all of which can be covered in this chapter (for example, important issues such as evidence acquisition and cyber forensic capability have not been discussed). For more detailed analysis of all issues see: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime.
31. An example of good practice that might be extended and developed more generally was the integrated approach to cybersecurity taken at the London Olympics (Interview, former UK cybercrime law enforcement official, July 2014).
32. An issue highlighted by Rob Wainwright, Director of Europol in his evidence to the UK House of Lords Committee on the next JHA programme (House of Lords, EU committee, 13th Report of Session 2013–2014, p.17). Indeed he called for greater policy coherence across the EU's cybersecurity policies.
33. Focal points are teams within Europol's Operations Department that are focussed on a specific category of crimes or criminal networks. They operate three focal point teams at present: Cyborg (high-tech crimes and malware), Twins (online child sexual exploitation) and Terminal (payment fraud).

6 Network and Information Security and Cyber Defence in the European Union

1. The EU has focused on self-protection (defence) given that it does not have, beyond what is provided by the member states, its own autonomous military capabilities. This is in contrast to the US which has focused developing cyber offensive capabilities in recent years.
2. The purpose of this communication was to revitalise and reinforce the European Commission original strategy document of 2001, 'Network and Information Security: proposal for a European Policy approach'.
3. The Council Conclusions on 'Prevention, Preparedness and Response to Terrorist Attacks' and the 'EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks' adopted by the Council in December

2004 endorsed the intention of the Commission to propose a EPCIP and CIWIN (Communication, EPCIP 2006).

4. Following a comprehensive review of the EPCIP and the Council Directive 2008/114/EC the European Commission (2013c) set out a new approach to the practical implementation of EPCIP through its three working streams – prevention, preparedness and response. Such a new approach sought to in particular take into account and address the interdependencies between critical infrastructures industry and state actors.
5. The Directive also advocated general risk management guidelines ('operator security plans'), security liaison officers and mandatory reporting, as well as the exchange of sensitive information among law enforcement authorities.
6. See also the European Parliament Resolution (2012) which endorsed the Commission's communications but also made additional recommendations which were taken on board in the EUCSS (2013) and the proposed NIS Directive (European Commission 2013a).
7. See ENISA for an up-to-date assessment of CERTs: http://www.enisa.europa.eu/activities/cert.
8. This was fully established in September 2012 after a one year pilot phase and serves all EU institutions, agencies and bodies. See: http://cert.europa.eu/cert/plainedition/en/cert_about.html.
9. The feasibility study for this undertaken by ENISA concluded 'that the most effective level of involvement for the European Union in the establishment and operation of an information sharing system for its home-users and SMEs would be that of a facilitator, moderator of discussion and a "keeper of good practice" '. Progress on its actual evolution and implementation has been slow, not least because of different perspectives among stakeholders on what this should entail. For details see: http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder.
10. France, Germany, Hungary, Italy, Netherlands, Sweden and UK.
11. The EP3R was founded through a non-paper which attempted to set out the goals of the Pubic Private Partnership (PPP), its purpose and its structure: See http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.ht.
12. Note, though, that this does not imply that the work of the EP3R was redundant. For example, the work on botnets was instructive and ENISA is undertaking a second review of EP3R to ascertain overall utility and lessons learnt.
13. For example, the priority area of developing industrial and technological resources for cybersecurity/promoting a single market for cybersecurity products.
14. There are three main working groups: working group 1 on risk management; working group 2 on information sharing/incident coordination; and working group 3 on Secure ICT Research and Innovation. The author was a participant member of working group 3.
15. A third exercise was planned for 2014. Whilst the technical aspect of the exercise took place in April 2014 (phase 1) there is no publically available information on the operational/tactical and strategic/political phases which were due to take place in the latter part of 2014. The objectives of Cyber Europe 2014 included: testing of the existing

standard cooperation procedures and mechanisms for managing cyber-crises in Europe; enhance national-level capabilities; explore the existing cooperation between the private and public sector; analyse the escalation and de-escalation processes (technical, operational and strategic level); understand the public affairs issues linked to large scale cyber-attacks. See: http://www.enisa.europa.eu/media/press-releases/biggest-eu-cyber-security-exercise-to-date-cyber-europe-2014-taking-place-today.

16. For example, the ENISA Good Practice Guide on National Exercises (2010).
17. According to the ENISA report, 'Participants from 30 countries (EU and EFTA) were represented in CYBER EUROPE 2010; 22 countries were actively playing, whilst eight countries were present as observers, having access to exercise happenings and findings. There was a central exercise control organisation in place, Exercise Control (EXCON), situated in Athens, which provided direction and guidance for the exercise. EXCON included the MS-moderators, one representative from each participating country, and the EXCON-moderators, ENISA and JRC, which had overall control of the exercise (ENISA, 2011a, p.6).
18. There has also been greater support by the Commission for an inclusion of democratic states such as India and Brazil in such structures in order to improve transparency and representation (see Chapter 7).
19. An impact assessment was carried out which considered, alongside the regulatory approach taken: 1. maintaining the status quo through a market/voluntary approach 2. A mixed approach combining a voluntary approach for member states in improving their capability and more regulatory requirements for private actors and public administrations (European Commission 2013b).
20. The UK government also pushed strongly for the removal of 'Internet Enablers' from the Directive.
21. Not all member states participate – some because they have opted out of cooperation in this area (Denmark), some because of lack of resource (Malta) and others through choice – because they believe it to be a national not European competence (UK) (Interview, EDA official, September 2014).
22. Note, there is a classified and unclassified version of the report. Findings reported here are from the publically available unclassified report; with the classified report including much more detail and in depth analysis of EU and EU MS cyber defence capability.
23. Derived from a commonly understood military framework of functional contributors to defence capability known as Defence Lines of Development (Robinson et al. 2013).
24. As well as the Cyber Ranges project, a pilot project was established to train and certify military students in Digital Forensics'; a pilot exercise in cooperation with Portugal and Estonia was set up on Cyber Strategic Decision Making; and there are also various other ad hoc projects, for instance, one on developing a situational awareness kit to provide a standardised cyber defence planning and management system, and another on Advanced Persistent Threat Detection.
25. For example, by establishing processes and mechanisms for integrating Cyber Threat Intelligence into Military Operations (for this, see Roehrig 2014).

26. The Smart Defence projects in cyber defence, so far, include the Malware Information Sharing Platform (MISP), the Smart Defence Multinational Cyber Defence Capability Development (MN CD2) project, and the Multinational Cyber Defence Education and Training (MN CD E&T) project (see NATO (2014) http://www.nato.int/cps/en/natohq/topics_78170.htm).

7 Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience?

1. ICANN is a private, US, not-for-profit, corporation that performs the functions of the Internet Assigned Names Authority (IANA) through which it constructs standards for the use and protection of names in cyberspace.
2. See https://ec.europa.eu/digital-agenda/en/global-internet-policy-observatory-gipo.
3. For an insightful view on the early impact of the Obama administration's cybersecurity proposals, see Hathaway (2011).
4. See also the specific work done by ENISA on critical infrastructure: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services.
5. This voluntary approach was embedded in the Cybersecurity Enhancement Act (S.1353) that was passed by the US Senate on 11 December 2014 and which became public law no.: 113–274 on 18 December 2014. See https://www.govtrack.us/congress/bills/113/s1353.
6. The EU, of course, had already conceived of a strategy to enhance the use of cloud in Europe prior to Snowden, which was mainly driven by a single market, economic logic. See: European strategy for Cloud computing – unleashing the power of cloud computing in Europe (2012). See also http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing.
7. Europeans who are not resident in the U.S. do not benefit from the safeguards of the 1974 US Privacy Act. See http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm).
8. For how EU data protection reform addresses fears of surveillance see http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.
9. For the General Data Protection Regulation text adopted by the European Parliament, see: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.
10. More accurately, the UK re-constituted the Draft Data Communications Bill (more generally labelled the Snoopers Charter by many rights groups in the UK). It was reinvented as the Data Retention and Investigatory Powers Act and became law on 17 July 2014. See https://www.liberty-human-rights.org.uk/campaigning/no-snoopers-charter.
11. It initially started with 48 countries.
12. See, for example, Ashford (2015).

References

ACPO e-crime Strategy (2009), Association of Chief Police Officers of England, Wales and Northern Ireland. Available at: http://www.acpo.police.uk/documents/crime/2009/200908CRIECS01.pdf (accessed October 2014).

'A Global Alliance Against Child Sexual Abuse Online' (2015), Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm (accessed February 2015).

Albrecht, P. J. (2015), 'EU General Data Protection Regulation: State of Play and 10 Main Issues', *LIBE, The Greens in the European Parliament*, 7 January 2015.

Alden, E. (2014), 'How Obama's NSA Reforms Could Help TTIP', *Council on Foreign Relations*, 15 January 2014.

Ashford, W. (2015), 'China and US Cross Swords Over Software Backdoors', *Computerweekly.com*, 5 March 2015. Available at: http://www.computerweekly.com/news/2240241750/China-and-US-cross-swords-over-software-backdoors?asrc=EM_EDA_40356910&utm_medium=EM&utm_source=EDA&utm_campaign=20150305_China%20and%20US%20cross%20swords%20over%20software%20backdoors_ (accessed March 2015).

Aspects of Identity Yearbook 2011–2012 (2011), BCS: The Chartered Institute for IT, Identity Assurance Working Group.

Bada, M., Creese, S., Goldsmith, M., Mitchel, C. and Phillips, E. (2014), 'Computer Emergency Response Teams (CERTs): An Overview', *Global Cyber Security Capacity Centre*. Available at: http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CERTs%20An%20Overview%20.pdf (accessed December 2014).

Bendiek, A. (2014), 'Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance and Data Protection', Stiftung Wissenschaft und Politik (SWP), SWP Research Paper, Berlin, March 2014.

Bendrath, R., Eriksson, J. and Giacomello G. (2007), 'Cyberterrorism to Cyberwar, Back and Forth: How the United States Securitized Cyberspace', in Eriksson, J. and Giacomello G. (eds.) *International Relations and Security in the Digital Age*, London, Routledge, pp.57–82.

Bendrath, R., Eriksson, J. and Giacomello, G. (2010), 'From "cyberterrorism" to "cyberwar", Back and Forth: How the United States Securitized Cyberspace', in Eriksson, J. and Giacomello, G. (eds.) *International Relations and Security in the Digital Age*, London and New York: Routledge.

Benkler, Y. (1998), 'The Commons as a Neglected Factor of Information Policy'. Available at: www.benkler.org/commons.pdf (accessed June 2013).

Benkler, Y. (2007), 'The Battle over the Institutional Ecology of the Digital Environment'. Available at: http://cyber.law.harvard.edu/wealth_of_networks/11._The_Battle_Over_the_Institutional_Ecology_of_the_Digital_Environment (accessed March 2015).

Bersick, S., Christou, C. and Yi, S. (forthcoming 2015), 'Cyber Security and EU-China Relations', in Kirchner, Emil, Christiansen, Thomas and Dorussen, Han

(eds.) *Security Relations between China and the European Union: From Convergence to Cooperation?* Cambridge: Cambridge University Press.

Betz, D. and Stevens, T. (2011), *Cyberspace and the State: Towards a Strategy for Cyber-Power*, The International Institute for Strategic Studies, Oxon: Routledge.

Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Ragazzi, F. and Scherrer, A. (2013), National Programmes for Mass Surveillance of Personal Data in EU Member States and their compatibility with EU Law, Directorate General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, European Parliament.

Boehm, F. and Cole, D. M. (2014), 'Data Retention After the Judgement of the European Court of Justice of the EU', The Greens/European Free Alliance, 30 June 2014. Available at: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_June_2014.pdf (accessed February 2015).

Bowden, C., Bigo, D. and Scherrer, A. (2013) The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights, Directorate General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, European Parliament.

Boyden, S. (1987), *Western Civilization in Biological Perspective: Patterns in Biohistory*, Oxford: Clarendon.

Brand, F. S. and Jax, K. (2007), Focusing the meaning(s) of resilience: Resilience as a descriptive concept and a boundary object. *Ecology and Society*, 12(1): 23. [online] Available at: http://www.ecologyandsociety.org/vol12/

Brassett, J. and Vaughan-Williams, N. (2015), 'Security and the Performative Politics of Resilience: Critical Infrastructure Protection and Humanitarian Emergency Preparedness', *Security Dialogue*, 46(1), 32–50.

Brewster, T. (2014), 'UK Forges Closer Cyber Ties with China Despite "endemic espionage" ', *The Guardian, Secure + Protect*, 18 June 2014.

Brown, I. and Marsden, C. T. (2007), 'Co-regulating Internet Security: The London Action Plan', http://essex.academia.edu/ChrisMarsden/Papers/700007/Co-regulating_Internet_security_the_London_Action_Plan (accessed October 2012).

Bygrave, A. L. (2013), 'Transatlantic Tensions on Data Privacy', *Transworld*, Working Paper 19, April 2013.

Castells, M. (1996), *The Information Age: Economy, Society and Culture, vol.1: The Rise of the Network Society*, Malden, MA: Blackwell.

Castells, M. (1997), *The Information Age: Economy, Society and Culture, vol.2: The Power of Identity*, Malden, MA: Blackwell.

Castells, M. (1998), *The Information Age: Economy, Society and Culture, vol.3: End of Millennium*, Malden, MA: Blackwell.

Chan, C. (2013), 'Leaked Documents Detail the Cyber Operations of US Spy Agencies'. Available at: http://gizmodo.com/leaked-documents-detail-the-cyber-operations-of-us-spy-1230265977 (accessed January 2015).

Chmutina, K., Bosher, L., Coaffee, J. and Rowlands, R. (2014), 'Towards Integrated Security and Resilience Framework: A Tool for Decision-Makers', *Procedia Economics and Finance*, 12/2014, DOI: 10.1016/S2212-5671(14)00909-5.

Christou, G. (2014), 'The EU's Approach to Cyber Security,' EU-China Security Cooperation: Performance and Prospects Project, Jean Monnet Multilateral Research Group'. Available at: http://privatewww.essex.ac.uk/~susyd/EUSC/publications.htm (accessed January 2015).

Christou, G. and Croft, S. (2012), *European Security Governance*, Oxon: Routledge.

Christou, G., Croft, S., Ceccorulli, M. and Lucarelli, S. (2010), 'European Union Security Governance: Putting the Security back In', *European Security*, Special Issue, 19 (3), September 2010, 341–361.

Christou, G. and Simpson, S. (2012), 'The Influence of Global Internet Institutions on the EU', in Costa, O. and Jørgensen, K. E. (eds.) *The Influence of International Institutions on the European Union*, Houndmills, Basingstoke: Palgrave MacMillan.

Christou, G. and Simpson, S. (2011), 'The European Union, Multilateralism and the Global Governance of the Internet', *Journal of European Public Policy*, 18(2), 241–257.

Christou, G. and Simpson, S. (2007), *The New Electronic Marketplace: European Governance Strategies in a Globalising Economy*, London: Edward Elgar.

China and Russia's 'International Code of Conduct for Information Security', Available at: http://news.dot-nxt.com/2011/09/13/china-russia-security-code-of-conduct (accessed October 2013).

Cirlig, C. C. (2014), 'Cyber Defence in the EU: Preparing for Cyber Warfare?', European Parliamentary Research Service, European Parliament Briefing, October 2014.

Clarke, A. R. and Knake, R. K. (2010), *Cyber War: The Threat to National Security and What to Do About It*, New York: Harper Collins.

Clarke, A. R. et al. (2013), 'Liberty and Security in a Changing World', Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, The Whitehouse, 12 December 2013. Available at: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed February 2015).

Coaffee, J. and Fussey, P. (2015), 'Constructing Resilience Through Security and Surveillance: The Politics, Practices and Tensions of Security-Driven Resilience', *Security Dialogue*, 46(1), 3–14.

Colarik, A. M. (2006), *Cyber Terrorism: Political and Economic Implications*, IGI Publishing.

Comfort, K. L., Boin, A. and Demchak, C. C. (eds.) (2010), *Designing Resilience: Preparing for Extreme Events*, Pittsburgh: University of Pittsburgh Press.

Cornish, P., Livingstone, D., Clemente, D. and York, C. (2011), 'Cyber Security and the UK's Critical National Infrastructure', *A Chatham House Report*, Chatham House, September 2011.

Council of the European Union (2011), 'Council Conclusions on Critical National Infrastructure Protection – 'Achievements and Next Steps: Towards Global Cyber-Security', 3093rd Transport, Telecommunications and Energy Council Meeting, Brussels, 27 May 2011.

Council of the European Union (2008a), 'Council Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection', Council Directive 2008/114/EC, 8 December 2008.

Council of the European Union (2008b), Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matter.

Council of the European Union (2005), Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems.

Council of the European Union (2004), Council Framework Decision 2004/68/JHA of 22 December 2003 on Combating the Sexual Exploitation of Children and Child Pornography.

Council of the European Union (2001), 2001/220/JHA: Council Framework Decision of 15 March 2001 on the Standing of Victims in Criminal Proceedings.

Cybercrime@IPA project of the Council of Europe and the European Union (2011), 'Specialised Cybercrime Units: Good Practice Study', Version 9 November 2011. Available at: www.coe.int/cybercrime (accessed May 2014).

'Cyber Crime Strategy' (2010), Home Office, CM7842, March 2010.

Cyber Defence Fact Sheet (2013), 'European Defence Agency'. Available at: http://www.eda.europa.eu (accessed August 2014).

'Cyber Essentials Scheme: Requirements for Basic Technical Protection Against Cyber Attacks' (2014), 'HM Government', June 2014. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf (accessed October 2014).

Cyber Security Building Resilience, Reducing Risks (2014), Chatham House, The Home of the Royal Institute of International Affairs, Conference, 19–20 May 2014.

'Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace' (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7 February 2013, JOIN (2013) 1 final.

'Cyber Security Strategy of the UK: Safety, Security and Resilience in Cyberspace' (2009), Office of Cyber Security and UK Cyber Security Operations Centre, June 2009.

Deauville Declaration (2011). Available at: http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html (accessed March 2015).

De Bruijne, M., Boin, A. and van Eeten, M. (2010), 'Resilience: Exploring the Concept and Its Meanings', in Comfort, L., Boin, A. and Demchal, C. (eds.) *Designing for Resilience: Preparing for Extreme Events*, Pittsburgh: Pittsburgh University Press.

Defence Cyber Protection Partnership (2015), Available at: https://www.adsgroup.org.uk/pages/65757387.asp.

Deibert, R. J., Rohozinski, R. and Crete-Nishihita, M. (2012), 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War', *Security Dialogue*, 43(1), 3–24.

Deibert, R. J., Palfrey, J. G., Rohozinski, R. and Zittrain, J. (eds.) (2011), *Access Contested: Security, Identity and Resistance in Asian Cyberspace*, Cambridge: MIT Press.

DG Home Affairs (2013), Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/child-sexual-abuse/index_en.htm (accessed March 2013).

Di Camillo, F. and Miranda, V. (2011), 'Ambiguous Definitions in the Cyber Domain: Costs, Risks, and the Way Forward', *IAI Working Papers* 1126, September 2011.

'Digital Britain' (2009), Final Report, June 2009. Department for Culture Media and Sport and Department for Business, Innovation and Skills. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228844/7650.pdf (accessed October 2014).

Downing, E. (2011), 'Cyber Security – A New National Programme', Science and Environment Section, SN/SC/5832, House of Commons Library, 23 June 2011.

Drewer, D. and Ellermann, J. (2012), 'Europol's Data Protection Framework as an Asset in the Fight Against Cybercrime', Europol, 19 November 2012. Available at: https://www.europol.europa.eu/content/publication/europols-data-protection-framework-asset-fight-against-cybercrime-1838 (accessed February 2014).

Dunn Cavelty, M. (2014), 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities', *Journal of Science and Engineering Ethics*, DOI: 10.1007/s11948-014-9551-y.

Dunn Cavelty, M. (2013), 'A Resilient Europe for an Open, Safe and Secure Cyberspace', Occasional Papers, No. 23, The Swedish Institute of International Affairs.

Dunn, M. (2010), 'Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory', in Eriksson, J. and Giacomello, G. (eds.) *International Relations and Security in the Digital Age*, London and New York: Routledge.

Dunn Cavelty, M. (2008a), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London and New York: Routledge.

Dunn Cavelty, M. (2008b), 'Critical (Information) Infrastructure Protection: History, Trends and Concepts', Centre for Security Studies, Swiss Federal Institute of Technology.

Dunn Cavelty, M. (2007), 'Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', *Journal of Information Technology and Politics*, 4(1), 19–35.

Dunn Cavelty, M. and Prior, T. (2013), 'Resilience in Security Policy: Present and Future', CSS Analysis in Security Policy, ETH Zurich, No. 142, October 2013.

ENISA Threat Landscape Report (2014), 'ENISA, Greece'. Available at: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape#b_start=0 (accessed January 2015).

ENISA, Press Release (26 June 2014), Available at: http://www.enisa.europa.eu/media/press-releases/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol (accessed March 2014).

ENISA (2008), 'Stock Taking of Member States', Policies and Regulations Related to Resilience of Public eCommunications Networks', ENISA, 2008.

ENISA (2013), '8th ENISA Workshop "CERTs in Europe" ', Report, ENISA, Greece.

ENISA (2012), 'On National and International Cyber Security Exercises: Survey, Analysis and Recommendations', ENISA, October 2012. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report-1.

ENISA (2012a) 'The Fight Against Cybercrime – Cooperation Between CERTs and Law Enforcement Agencies to Fight Against Cybercrime', ENISA, February 2012.

ENISA (2012b) 'Give and Take: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime. Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders', ENISA, November 2012.

ENISA (2012c), 'Cyber Europe 2012: Key Findings and Recommendations', ENISA, December 2012. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report (accessed July 2014).

ENISA (2011), 'A Flair for Sharing – Encouraging Information Exchange Between CERTs', ENISA, November 2011.

ENISA (2011a), 'Cyber Europe 2010 Evaluation Report', ENISA. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010/ce2010report (accessed July 2014).

ENISA (2011b), 'Proactive Detection of Network Incidents', ENISA Report. Available at: https://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report (accessed July 2014).

ENISA (2011c), *Inter-X: Resilience of the Internet Interconnection Ecosystem*, Summary Report, ENISA April 2011.

ENISA (2011d), *Cooperative Models for Effective Public-Private Partnerships: Good Practice Guide*, ENISA 2011.

ENISA (2010), 'ENISA Good Practice Guide on National Exercises', ENISA. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce (accessed July 2014).

Eriksson, J. (2001), Cyberplagues, IT and Security: Threat Politics in the Information Age, *Journal of Contingencies and Crisis Management*, 9(4), 211–222.

Eriksson, J. and Giacomello G. (eds.) (2010) *International Relations and Security in the Digital Age*, London and New York: Routledge.

EU Kids Online Survey (2010), 'Risks and Safety for Children on the Internet: The UK Report'. Available at: http://eprints.lse.ac.uk/33730/ (accessed April 2014).

Europe 2020 (2010), 'A Strategy for Smart, Sustainable and Inclusive Growth', European Commission, COM (2010) 2020, 3 March 2010.

European Commission (2014), EU-US Fact Sheet: Negotiations on Data Protection, Brussels, June 2014. Available at: http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf (accessed February 2015).

European Commission (2013), 'Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement and Training (Europol) and Repealing Decisions 2009/371/JHA and 2005/681/JHA', Brussels, 27 March 2013, COM (2013) 173 final, 2013/0091 (COD).

European Commission (2013a), 'Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level of Network and Information Security Across the Union', Brussels 7, February 2013, COM (2013) 48 final.

European Commission (2013b), 'Impact Assessment', Accompanying the Document Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level of Network and Information Security Across the Union, Commission Staff Working Document, Strasbourg, 7 February 2013, SWD(2013) Final.

European Commission (2013c), Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures More Secure, SWD (2013) 318 Final, Brussels, 28 August 2013.

European Commission (2013d), 'Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU', Brussels, 27 November 2013, COM (2013) 847 final.

European Commission (2013e), 'Restoring Trust in EU-US Data Flows', Memo, Brussels, 27 November 2013. Available at: http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm (accessed February 2015).

European Commission (2012), Communication from the Commission to the Council and the European Parliament, 'Tackling Cybercrime in Our Digital Age: Establishing a European Cybercrime Centre', COM (012) 140 final, Brussels, 28 March 2012.

European Commission (2011), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and Next Steps: Towards Global Cyber-security', COM (2011) 163 final, Brussels, 31 March 2011.

European Commission (2011), 'Proposal on a European Strategy for Internet Security', November 2011. Available at: http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf (accessed September 2013).

European Commission (2011), 'Cyber security: EU and US Strengthen Transatlantic Cooperation in Face of Mounting Global Cyber-Security and Cybercrime Threats', Brussels, 14 April 2011. Available at: http://europa.eu/rapid/press-release_MEMO-11-246_en.htm (accessed January 2015).

European Commission (2010), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'A Digital Agenda for Europe', COM (2010) 245 final/2, 26 August 2010.

European Commission (2009a), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, 'Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience', COM (2009) 149 final, Brussels, 30 March 2009.

European Commission (2009b), 'Internet Governance: Next Steps', Communication from the Commission from the European Parliament and the Council, Brussels, COM (2009) 277 final, 18 July 2009.

European Commission (2008), COM (2008) 448: Report from the Commission to the Council Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks Against Information Systems.

European Commission (2006a), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'A strategy for a Secure Information Society – "Dialogue, Partnership and Empowerment" ', COM (2006) 251 Final, Brussels, 31 May 2006.

European Commission (2006b), Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM (2006) 786 Final, Brussels, 12 December 2006.

European Commission (2005), Green Paper on the European Programme for Critical Infrastructure Protection, COM (2005) 576 Final, Brussels, 17 November 2005.

European Commission (2005), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'i2010 – A European Information Society for growth and employment', COM (2005) 229 Final, Brussels, 1 June 2005.

European Commission (2001a), 'Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-Related Crime', COM (2000) 890, 26 January 2001.

European Commission (2001b), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Network and Information Security: Proposal for A European Policy Approach, COM (2001) 298 Final, Brussels, 6 June 2001.

European Commission (1999), Communication of 8 December 1999 on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000 – eEurope – An Information Society for All, COM (1999) 687 Final (not published in the Official Journal).

European Council Conclusions (19–20 December 2013), Available at: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/140214.pdf (accessed July 2014).

European Cybercrime Centre (EC3) First Year Report (2014), Europol. Available at: http://www.europol.org (accessed December 2014).

European Digital Rights Initiative (2011), 'The Slide from "Self-Regulation" to Corporate Censorship', January 2011. Available at: http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf (accessed March 2014).

European Frontier Foundation (2011), Available at: https://www.eff.org/issues/mandatory-data-retention/eu (accessed March 2014).

European Parliament (2013), Draft Report, 'On the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens of Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs' (2013/2188 (INI)), Committee on Civil Liberties, Justice and Home Affairs. Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/moraes_1014703_/moraes_1014703_en.pdf (accessed February 2015).

European Parliament (2012), Report on Critical Information Infrastructure Protection – Achievements and Next Steps: Towards Global Cyber-Security', Committee on Industry, Research and Energy, RR\902472EN.doc, 16 May 2012.

European Parliament (2011), On the Proposal for a Directive of the European Parliament and of the Council on Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA, (COM(2010)0094 – C7-0088/2010 – 2010/0064(COD)), Draft Report, {LIBE}Committee on Civil Liberties, Justice and Home Affairs, 24 January 2011. Available at: http://www.europarl.europa.eu/sides/getDoc.do?

type=COMPARL&mode=XML&language=EN&reference=PE452.564 (accessed March 2014).

European Parliament and the Council (2013), Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA.

European Parliament and the Council (2012), Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 Establishing Minimum Standards on the Rights, Support and Protection of Victims of Crime, and Replacing Council Framework Decision 2001/220/JHA.

European Parliament and the Council (2012), Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 Establishing Minimum Standards on the Rights, Support and Protection of Victims of Crime, and Replacing Council Framework Decision 2001/220/JHA.

European Parliament and the Council (2011), Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA.

European Parliament and Council (2009), Regulation (EC) No 544/2009 of the European Parliament and of the Council of 18 June 2009 Amending Regulation (EC) No 717/2007 on Roaming on Public Mobile Telephone Networks Within the Community and Directive 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services.

European Parliament and the Council (2002), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).

European Parliament and the Council (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.

EU Prepares to Launch First Cybercrime Centre (2012), EuroActiv, 29 March 2012. Available at: http://www.euractiv.com/infosociety/eu-prepares-launch-cybercrime-ce-news-511823 (accessed March 2015).

European Principles and Guidelines for Internet Resilience and Stability (2011), Available at: http://ec.europa.eu/danmark/documents/alle_emner/videnskabelig/110401_rapport_cyberangreb_en.pdf (accessed March 2013).

European Security Research Innovation Forum Final Report (2009), Available at: http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (accessed March 2014).

European Strategy for Cloud Computing – Unleashing the Power of Cloud Computing in Europe (2012), Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF (accessed March 2015).

EU-US Cooperation on Cybersecurity and Cyberspace (2014), Fact Sheet, European External Action Service, 26 March 2014.

EU-US Working Group on Cybersecurity and Cybercrime (2011), Concept Paper, European Commission, 13 April 2011.

Flyverbom, M. (2011), *The Power of Networks: Organizing the Global Politics of the Internet*, Cheltenham: Edward Elgar Publishing

Gellman, B. and Nakashima, E. (2013), 'US Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show', *Washington Post*, 30 August 2013. Available at: http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html (accessed January 2015).

Gjelten, T. (2010), Seeing the Internet as an 'Information Weapon', 23 September 2010, Available at: http://www.npr.org/templates/story/story.php?storyId=130052701 (accessed September 2013).

Goldsmith, J. (2011), *Cybersecurity Treaties: A Skeptical View, Future Challenges Essay*, Hoover Institution, Stanford University.

Greenwald, G. and MacAskill, E. (2013), Obama Orders US to Draw up Overseas Target List for Cyber Attacks, *The Guardian*, 7 June 2013.

Grimm, V. and Calabrese, J. M. (2011), 'What Is Resilience? A Short Introduction', in Deffuant, G. and Gilbert, N. (eds.) *Viability and Resistance of Complex Systems: Concepts, Methods and Case Studies*, Springer.

Hague, W. (2011), 'Security and Freedom in the Cyber Age – Seeking the Rules of the Road', Speech Given to the Munich Security Conference, 4 February 2011.

Hallenberg, J., Sperling, J. and Wagnsson, C. (2009), *European Security Governance: The European Union in a Westphalian World*, London: Routledge.

Handmer, J. W. and Dovers, S. R. (1996), 'A Typology of Resilience: Rethinking Institutions for Sustainable Development', *Organization & Environment*, 9, 482–511.

Hart, A. G. (2001), 'The G8 and the Governance of Cyberspace', in Fratianni, M. (ed.) *New Perspectives on Global Governance: Why America Needs the G8*, Aldershot: Ashgate Publishing Limited.

Hathaway, M. (2011), 'Examining the Homeland Security Impact of the Obama Administrations Cybersecurity Proposal', Statement Before the House off Representative Committee on Homeland Security, Sub-Committee on Cybersecurity, Infrastructure Protection and Security Technologies, 24 June 2011.

Healey, J. (2011a), 'Comparing Norms for National Conduct in Cyberspace', 20th September 2011. Available at: http://www.acus.org (accessed October 2013).

Healey, J. (2011b), 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms', 21 September 2011. Available at: http://www.acus.org (accessed October 2013).

Hern, B. (2014), 'British Government "breaking law" in Forcing Data Retention by Companies', theguardian.com, 24 June 2014. Available at: http://www.theguardian.com/technology/2014/jun/24/british-government-breaking-law-in-forcing-data-retention-by-companies (accessed February 2015).

Herrington, L. and Aldrich, R. (2012), 'The Future of Cyber-Resilience in an Age of Global Complexity', *Politics*, 33(4), 299–310.

Hilley, S. (2005), 'Pressure Mounts on US Senate to Pass Cyber Crime Treaty', *Digital Investigation*, 2, 171–174.

Holling, C. (1973), 'Resilience and the Sustainability of Ecological Systems', *Annual Review of Ecology and Systematics*, 4(1), 1–23.

Hosein, I. and Eriksson, J. (2010), 'International Policy Dynamics and the Regulation of Data Flows: Bypassing Domestic Restrictions', in Eriksson, J. and Giacomello, G. (eds.) *International Relations and Security in the Digital Age*, London and New York: Routledge.

House of Lords, EU Committee 13th Report of Session 2013–2014, 'Strategic guidelines for the EU's next Justice and Home Affairs Programme: Steady as She Goes', HL Paper 173, House of Lords, April 2014. Available at: http://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-home-affairs-sub-committee-f-/inquiries/parliament-2010/rome-programme/ (accessed July 2014).

House of Lords (2010–2011), Government and Commission Responses Session: 2009–2010, European Union Committee, 4th Report of the 2010–11 Session, UK Government.

House of Lords EU Committee Report (2010), 'Protecting Europe Against Large Scale Cyber Attacks', HL Paper 68, 2009–2010, March 2010, para 24.

Improvements Proposed for Europol (2013), Available at: http://www.eubusiness.com/topics/crime/europol-2, 27 March 2013 (accessed July 2014).

Information Assurance Advisory Council Symposium, 'Securing the Cloud – Securing Me', Royal College of Physicians, London, 12 September 2012.

International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World (2011), The White House, Washington DC, May 2011.

International Telecommunications Union (ITU) (2011) National Cybersecurity Strategy Guide, ITU, September 2011.

International Telecommunications Union (ITU) (2008) Global Cybersecurity Agenda, High level Experts Group, Global Strategic Report, ITU.

International Telecommunications Union (ITU) (2008a) Q.22/1 Report on Best Practices for a National Approach to Cyber Security: A Management Framework for Organizing National Cybersecurity Efforts (2008), ITU-D Secretariat, January 2008.

Janczewski, L. J. and Colarik, A. M. (2007), *Cyber Warfare or Cyber Terrorism*, USA: IGI Global.

Janczewski, L. J. and Colarik, A. M. (2008), *Cyber Warfare and Cyber Terrorism*, USA: Information Science Reference, IGI Global.

Jeffray, C. (2014), 'Five Unanswered Questions on the UK's New Computer Emergency Response Team', RUSI Analysis, RUSI, UK.

Joint Statement of the EU-US Summit 2010, 20 November 2010, Lisbon. Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/597&type=HTML (accessed February 2015).

Karatzogianni, A. (ed.) (2009), *Cyber Conflict and Global Politics*, London and New York: Routledge.

Karatzogianni, A. (2006), *The Politics of Cyber Conflict*, London and New York: Routledge.

Kavalski, E. (2009), 'Timescapes of Security: Clocks, Clouds, and the Complexity of Security Governance', *World Futures*, 65(7), 527–551.

Kerry, C. (2014), 'Missed Connections: Talking with Europe About Data, Privacy, and Surveillance', Center for Technology Innovation, Brookings, May 2014.

Kirchner, J. E. and Sperling, J. (2007a), *Global Security Governance: Competing Perceptions of Security in the 21st Century*, London: Routledge.

Kirchner, J. E. and Sperling, J. (2007b), *European Union Security Governance*, Manchester: Manchester University Press.
Klimburg, A. (2012), 'The Internet Yalta', *Commentary, Center for New American Security*, 5 February 2013.
Klimburg, A. (2011a), 'Mobilising Cyber Power', *Survival*, 53(1), 41–60.
Klimburg, A. (2011b), 'Ruling the Domain: Self-Regulation and the Security of the Internet', Austrian Institute of International Affairs, Paper Distributed at the 11th Meeting of the ICANN Studienkreis, 28/29 April 2011.
Klimburg, A. and Tiirmaa-Klaar, H. (2011), 'Cyber War and Cyber Security: Challenges Faced by the EU and Its Member States', DG for External Policies, Policy Department, European Parliament, April 2011.
Krahman, E. (2003), 'Conceptualizing Security Governance', *Cooperation and Conflict*, 38(1), 5–26.
Kramer, F. D. Starr, S. and Wentz, K. L. (eds.) (2010), *Cyber Power and National Security*, Washington, DC: National Defence UP.
Kroes, N. (2011), 'I Don't Like to Be too Diplomatic. That Is Not My Style: Neelie Kroes Talks Internet Governance'. Available at: http://news.dot-nxt.com/2011/09/30/kroes-interview-igf (accessed June 2013).
Kruger, G. L. (2013), 'Internet Domain Names: Background and Policy Issues', Congressional Research Service Report, 7–5700. Available at: www.crs.gov (accessed November 2014).
Kshetri, N. (2013), *Cybercrime and Cybersecurity in the Global South*, New Political Economy Series, Houndmills, Basingstoke: Palgrave Macmillan.
Laprise, J. (2014), 'Internet Governance: The New "Great Game" ', The Centre for Global Communications Studies, University of Pennsylvania.
Lentzos, F. and Rose, N. (2009), 'Governing Insecurity: Contingency Planning, Protection, Resilience', *Economy and Society*, 38(2), 230–54.
Lewis, A. J. (2014), 'Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms', Strategic Technologies Program, Centre for Strategic and International Studies, Washington, DC, USA.
Leyden, J. (2011), 'EU Parliament Suspends Webmail After Cyber-Attack', *The Register*, 31 March 2011. Available at: http://www.theregister.co.uk/2011/03/31/eu_parliament_hack/ (accessed March 2015).
Libicki, M. C. (2009), *Cyber Deterrence and Cyber War*, Rand Corporation.
Libicki, M. C. (2007), *Conquest in Cyberspace: National Security and Information Warfare*, New York: Cambridge University Press.
Livingstone, S. (2013), 'A Better Internet for UK Children?', 23 April 2013. Available at: http://blogs.lse.ac.uk/mediapolicyproject/2013/04/23/a-better-internet-for-uk-children/ (accessed April 2014).
Long, W. (2014), 'What to Expect from the EU's NIS Directive', *Computer Weekly*. Available at: http://www.computerweekly.com/opinion/What-to-expect-from-European-NIS-Directive (accessed December 2014).
Malcolm, J. (2008), *Multi-Stakeholder Governance and the Internet Governance Forum*, Perth: Terminus Press.
Marion, E. N. (2010), 'The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation', *International Journal of Cyber Criminology*, 4 (Combined Issue 1&2), 699–712.
Mehan, J. (2008), *CyberWar, CyberTerror, CyberCrime*, Cambridgeshire: IT Governance Publishing.

Meyer, P. (2013), 'Cyber Security Takes the Floor at UN', Canadian International Council, 12 November 2013. Available at: http://opencanada.org/features/the-think-tank/comments/cyber-security-takes-the-floor-at-the-un/ (accessed January 2014).

Micek, P. and Masse, E. (2014), 'US May Grant Rights to EU Citizens Under Privacy Act', Access, 16 July 2014.

Mohan, R. (2011), DNSSEC Baby Steps Reported at ICANN 41, CircleID Internet Infrastructure, 29 July 2011.

Mowlana, H. (1997), *Global Information and World Communication: New Frontiers in International Relations*, London: Sage.

Mueller, M. L. (2010), *Networks and States: The Global Politics of the Internet*, MIT Press.

Net Losses: Estimating the Global Cost of Cybercrime (2014), Economic Impact of Cybercrime II, Center for Strategic and International Studies, McAfee/Intel Security, June 2014. Available at: http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf (accessed March 2015).

Neville-Jones, P. and Phillips, M. (2012), 'Where Next for UK Cyber-Security?' *RUSI Journal*, 157(6), Dec 2012, 32–40.

North Atlantic Treaty Organisation (NATO) (2014), Available at: http://www.nato.int/cps/en/natohq/topics_78170.htm (accessed December 2014).

Norton Cybercrime Report (2013), 'Symantec'. Available at: https://msisac.cisecurity.org/resources/reports/documents/b-norton-report-2013.pdf (accessed December 2014).

Noshiravani, R. (2011), *NATO and Cyber Security: Building on the Strategic Concept*, 20 May 2011, Rapporteur Report, The NATO Science for Peace and Security Programme, Chatham House.

Nye, J. (2010), 'Cyber Power', Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010.

Obama seeks $14 billion to boost US cybersecurity defences', Reuters, 15 February 2015. Available at: http://www.reuters.com (accessed January 2015).

OECD (2012), 'Proactive Policy Measures by Internet Service Providers Against Botnets', OECD Digital Economy Papers, No.199, OECD Publishing. Available at: http://dx.doi.org/10.1787/5k98tq42t18w-en (accessed July 2013).

OECD (2003), 'Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security', Working Party on Information Security and Privacy, DSTI/ICCP/REG(2003)5/REV1, Organisation for Economic Cooperation and Development, Paris, France.

OECD (2002), 'OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security', Organisation for Economic Cooperation and Development, Paris, France.

Office of the Director of National Intelligence (2015), Available at: http://icontherecord.tumblr.com/ppd-28/2015/overview.

O'Neill, M. (2012), 'Cyber Crime and Cyber Security: A Late Developer in the EU's AFSJ', *Draft Paper*, Presented at Cybercrime and Cyber Security Workshop, University of Abertray, Dundee, 10 September 2012.

P8 Experts Group on Transnational Organized Crime (Lyon Group): 40 Recommendations. Available at: http://www.auswaertiges-amt.de/cae/servlet/contentblob/357602/publicationFile/3516/G8-Lyon-40recomOCrime1996.pdf (accessed March 2015).

Pearse, R. Buckenham, P. and Donnelly, N. (2015), 'EU Network and Information Security Directive', Society for Computers and Law. Available at: http://www.scl.org/site.aspx?i=ed39127 (accessed February 2015).

'Pentagon Creates 13 Offensive Cyber Teams for Worldwide Attacks' (2013), RT, 13 March 2013. Available at: http://rt.com/usa/alexander-cyber-command-offensive-209/ (accessed January 2015).

Perl, R. (2010), 'Combating Terrorist Use of the Internet/Comprehensively Enhancing Cyber Security', Counter Terror Expo, 'Countering Terrorism in a Changing World', 14–15 April 2010, London, UK.

Porcedda, G. M. (2012), Data Protection and the Prevention of Cybercrime: The EU as an Area of Security? EUI Working Papers, Law 2012/25, Department of Law. Available at: http://cadmus.eui.eu/bitstream/handle/1814/23296/LAW-2012-25.pdf?sequence=1 (accessed March 2014).

Press Release, '1st EU-US Cyber Dialogue' (2014), Brussels, 5 December 2014.

Pritchard, R. (2013), 'UK Cyber Response: Getting It Right Matters', RUSI Analysis, RUSI.

Reding, V. (2013), Letter to the US Attorney General of the United States Department of Justice, 10 June 2013. Available at: http://www.statewatch.org/news/2013/jun/eu-usa-reding-ag.letter.pdf (accessed February 2015).

Report of the Global Alliance Against Child Sexual Abuse Online (2013), European Commission, DG Home Affairs, December 2013. Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_report_201312_en.pdf (accessed February 2015).

Robinson, N. (2014), 'EU Cyber-Defence: A Work in Progress', European Union Institute for Security Studies, March 2014.

Robinson, N. Walczak, A. Brune, S.-C. Esterle, A. Rodriguez, P. (2013), Stocktaking Study of Military Cyber Defence Capabilities in the European Union, RAND Europe Report Prepared for the European Defence Agency (UNCLASSIFIED SUMMARY REPORT).

Roehrig, W. (2014), 'How to Integrate Cyber Threat Intelligence into EU-led Military Operations', Cyber Intelligence Europe, Brussels, 23 September 2014.

Roehrig, W. (2013), 'Mainstreaming European Military Cyber Defence Training and Exercises', September 2013, 2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises, 23–24 September 2013.

Roehrig, W. and Smeaton, R. (2013), 'Cyber Security and Cyber Defence in the European Union: Opportunities, Synergies and Challenges', European Defence Agency.

Saran, C. (2014), 'European Parliament Calls to Drop Safe Harbour', ComputerWeekly.com, 16 January 2014. Available at: http://www.computerweekly.com/news/2240212616/European-parliaments-calls-to-drop-Safe-Harbour (accessed January 2015).

Schneider, V. (2012), 'Governance and Complexity', in Levi-Faur, D. (ed.) *The Oxford Handbook of Governance*, Oxford: Oxford University Press.

Schoon, I. (2010), (ed.) *Risk and Resilience: Adaptations in Changing Times*, Cambridge: Cambridge University Press.

Scott, M. (2010), 'With Three Months to go to DNSSEC, Someone's Fudging Root Zone Records', *Betanews*, March 2010. Available at: http://www.betanews.

com/article/with-three-months-to-go-to-DNSSES-someones-fudging-root-zone-records/1269642342 (accessed June 2013).
Shah, S. (2012), 'UK Cyber Security – Fragmented and Failing', *Computing*, 28 November 2012.
Shore, M., Du, Y. and Zeadally, S. (2011), 'A Public-Private Partnership Model for National Cybersecurity', *Policy & Internet*, 3(2), Art.8.
Sliwinski, F. K. (2014), 'Moving Beyond the European Union's Weakness as Cyber-Security Agent', *Contemporary Security Policy*, DOI: 10.1080/13523260.2014.959261 (22 September 2014).
Sofaer, D. A., Clarke, D. and Diffie, W. (2010), 'Cybersecurity and International Agreements', Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy. Available at: http://www.nap.edu/catalog/12997.html (accessed February 2015).
Sommer, P. and Brown, I. (2011), 'Reducing Systemic Cybersecurity Risk', OECD/IFP Project on 'Future Global Shocks', IFP/WKP/FGS(2011)3.
Stevens, T. (2012), 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 33(1), 148–170.
Szilecki, K. Pattberg, P. and Biermann, F. (2011), 'Explaining Variation in the Effectiveness of Transnational Energy Partnerships', *Governance: An International Journal of Policy, Administration and Institutions*, 24(4), 713–736.
Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), *Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge: Cambridge University Press.
'The Digital Economy: Potential, Perils and Promises' (2014), A Report of the Digital Economy Task Force, March 2014.
'The National Crime Agency: A Plan for the Creation of a National Crime Fighting Capability' (2011), Home Office, June 2011, CM 8097.
'The UK Cyber Security Strategy: Report and Forward Plans' (2014), Cabinet Office, December 2014.
'The UK Cyber Security Strategy: Landscape Review' (2013), Report by the Controller and Auditor General, HC 890, National Audit Office, 12 February 2013.
'The UK Cyber Security Strategy: Report and Forward Plans' (2013), Cabinet Office, December 2013.
'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World' (2011), Cabinet Office, November 2011.
Tick, E. (2010), Global Cyber Security – Thinking About the Niche for NATO, *The SAIS Review of International Affairs*, Fall 2010 (pre-publication).
Titch, S. (2013), 'US Cybersecurity Policy: Problems and Principles', *Policy Brief, the Heartland Institute*, August 2013.
Traynor, I. (2014), 'Internet Governance too US-centric, Says European Commission', 12 February 2014. Available at: http://www.theguardian.com/technology/2014/feb/12/internet-governance-us-european-commission (accessed January 2015).
'UK Cyber Security Progress Welcomed' (2013), Computer Weekly.com. Available at: http://www.computerweekly.com (accessed December 2013).
UK Department of Business Innovation and Skills (2013), Call For Evidence on Proposed EU Directive on Network and Information Security, Report on

Summary of Responses, September 2013. Available at: https://www.gov.uk/government/consultations/eu-directive-on-network-and-information-security-call-for-evidence (accessed July 2014).

UK Home Office (2013), 'The European Commission's Proposal for a Europol Regulation'. Available at: http://www.gov.uk/speeches/the-european-commissions-proposal-for-a-europol-regulation (accessed July 2014).

United Nations (2010), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201, Study Series 33, 2010.

'Update on the National Cyber Security Programme' (2014), Report by the Controller and Auditor General, HC 626, National Audit Office, 10 September 2014.

US-EU Cyber Cooperation FACT SHEET (2014), The White House, Office of the Press Secretary, 26.3.14. Available at: http://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation (accessed February 2015).

Valeri, L. (2010), 'Public-private Cooperation and Information Assurance', in Eriksson, J. and Giacomello, G. (eds.) *International Relations and Security in the Digital Age*, London and New York: Routledge.

Van der Steeg, D. (2011), 'IPv6 Security: Transition from IPv4 to IPv6', University of Twente, June 2011.

Venkatraman, A. (2013), 'EC urges Europe: Become a 'trusted cloud region' in the Post-PRISM Age', *Computer Weekly Europe*, December 2013.

Verton, D. (2003), *Black Ice: The Invisible Threat of Cyber-Terrorism*, California: McGraw-Hill Companies.

Volter, W. (2013), 'The UN Takes a Big Step Forward on Cybersecurity', *Arms Control Today*. Available at: https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity (accessed January 2014).

Walker, J. and Cooper, M. (2011), 'Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation', *Security Dialogue*, 42(2), 143–60.

Watt, N. (2013), 'Prism Scandal: European Commission to Seek Privacy Guarantees from US', *theguardian.com*, 10 June 2013. Available at: http://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees (accessed February 2015).

Weber, M. A. (2014), 'The Council of Europe's Convention on Cybercrime', *Berkeley Technology Law Journal*, 18(1). Available at: http://scholarship.law.berkeley.edu/btlj/vol18/iss1/28 (accessed 30 January 2014).

Webber, M. (2007), *Inclusion, Exclusion and the Governance of European Security*, Manchester and New York: Manchester University Press.

Webber, M. Croft, S. Howorth, J. Terriff, T. and Krahmann, E. (2004), 'The Governance of European Security', *Review of International Studies*, 30(3), 3–26.

Weinburg, J. (2010) 'Non-State Actors and Global Informal Governance – The Case of ICANN', Wayne State University Law School Research Paper No. 10-05. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621862 (accessed March 2015).

Wiemann, G. (2006), *Cyberterrorism: How Real Is the Threat*, Washington, DC: United States Institute of Peace.

Wildavsky, A. B. (1995), *But Is It True? A Citizen's Guide to Environmental Health and Safety Issues*, Cambridge, MA: Harvard University Press.

Wildavsky, A. B. (1988), *Searching for Safety*, New Brunswick: Transaction.
Yannakogeorgos, P. A. (2015), 'The Rise of IPv6: Benefits and Costs of Transforming Military Cyberspace', *Air and Space Power Journal*, 29(2), March–April 2015, 103–128.
Yannakogeorgos, P. A. and Lowther, A. B. (eds.) (2013), *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, London: CRC Press.

Index

Note: Locators followed by the letter 'n' refer to notes.