Cyber-security in the European Region:

Anticipatory Governance and Practices

A thesis submitted to The University of Manchester for the degree of
Doctor of Philosophy in the Faculty of Humanities
The School of Law

Tine Højsgaard Munk

2015

Supervisors:

1st Supervisor: Professor Dr Toby Seddon,
The University of Manchester
2nd Supervisor: Professor Dr Dora Kostakopoulou,
The University of Warwick

To Family and Friends

1 Table of Contents

Contents

1 Table of Contents ... 3
2 Abstract ... 7
3 Declaration ... 8
4 Copyright Statement ... 8
5 Acknowledgements ... 9
6 Abbreviation ... 10
7 Glossary ... 11

1 Introduction ... 12
1.1 Introduction ... 12
1.2 The Research Objectives ... 16
1.3 Aim and Scope of the Research: The Contribution to Existing Literature ... 19
1.4 Methodology ... 24
1.5 Structure of the Thesis ... 28

2 The Evaluation of Security; From Threat to Risk ... 30
2.1 Introduction ... 30
2.2 Conceptualising the Relationship between Threat and Security ... 31
2.2.1 Conceptualising Threats ... 32
2.2.2 Conceptualising Security ... 33
2.3 The Development of Security ... 36
2.3.1 The First World War ... 37
2.3.2 The Second World War ... 38
2.3.3 The Cold War ... 39
2.4 The Historical Shift in Analysing Security Post-Cold War ... 41
2.4.1 The ‘War on Terror’ ... 43
2.4.2 Risk-Security Paradigm ... 44
2.5 Emerging Security Issues in the 21st Century: The Concept of Cyber-security ... 46
2.6 Conceptualising Cyber-space Related Crime ... 47
2.6.1 The Typology of Cyber-crime ... 52
2.6.2 The Typology of Cyber-warfare ... 52
2.6.3 The Typology of Cyber-terrorism ... 54
2.7 Conclusion ... 56

3 Perspectives on Security Governance. Nodal Governance, the Concept of Risk, and the use of Anticipatory Governance ... 58
3.1 Introduction ... 58
3.2 The Theoretical Foundation for Cyber-security Governance ... 59
3.3 Governmentality and Nodal Governance ... 62
3.3.1 Nodal Governance ... 64
3.3.2 Indirect Governance ... 67
3.4 Risk, Anticipatory Governance and the Concept of Resilience ... 71
3.5 Conceptualising Risk ... 73
3.6 Defining Risk ... 75
3.7 Risk-Management ... 76
3.7.1 Risk Perception ... 77
3.7.2 Risk Assessment and Risk Categorisation ... 78
3.7.3 Governing Risks ... 79
3.8 Anticipatory Governance and Practices ... 82

3.8.1 Resilience and Preparedness....83
3.8.2 Preparedness and Continuity....87
3.8.3 Anticipatory Management Techniques....88
3.8.4 Risk-based and Threat-based Security Management....92
3.9 Conclusion....94

4 Two Security Schools and Synthesising the Theoretical Foundation....96
4.1 Introduction....96
4.2 Two Schools in Security: The Copenhagen School and the Paris School....97
4.3 Broadening and Deepening the Security Agenda....98
4.4 The Copenhagen School on Peace and Conflict....101
4.4.1 Exceptionalism and the State-centric Approach....102
4.4.2 The Speech-act, Securitization, and Desecuritization....104
4.5 Rethinking Securitization in the Internet Age....107
4.5.1 Hyper-securitization....107
4.5.2 Everyday Practices....108
4.5.3 Technification....109
4.6 The Paris School on Security....110
4.6.1 The Paris School and the Management of Unease....111
4.6.2 The Internal-External Nexus....113
4.6.3 Policing (In)Securities....115
4.6.4 Networked Structures....117
4.7 Comparing the Two Security Schools and their Influence on Anticipatory Governance and Practices....119
4.8 Synthesising a Theoretical Framework....122
4.8.1 Transnational and Cross-sectoral Cooperation....125
4.8.2 Security Actors and Cooperation....126
4.8.3 Anticipatory Governance....128
4.8.4 Anticipatory Governance and Regulatory Practices....129
4.9 Methodology....131
4.9.1 Identifying the Area....132
4.9.2 Data collection....133
4.9.3 Analysing Significant Anticipatory Governance Structures....134
4.10 Conclusion....134

5 European Cyber-security Governance....136
5.1 Introduction....136
5.2 The Emerging Risk of Cyber-crime....137
5.3 Cyber-security Cooperation and Nodal Governmentality....139
5.4 Transnational Cooperation....142
5.4.1 International Cooperation....143
5.4.2 The Council of Europe and the Convention on Cyber-crime....146
5.4.3 The EU and Regional Cyber-crime Cooperation....147
5.5 Cross-sectoral Cooperation in the European Region....151
5.5.1 The CoE and Cross-sectoral Cooperation....153
5.5.2 The EU and Cross-sectoral Cooperation....154
5.5.3 The EU's Public-Private Partnerships....155
5.5.4 Engaging Public and Private Sectors....157
5.6 Oversight, Transparency and Accountability in Cyber-security Governance....159
5.7 Anticipatory Governance and the Development of Rules, Practices and Processes....161
5.7.1 State Regulation....163
5.7.2 Technical Regulation....164
5.7.3 Awareness-raising and Education....167
5.7.4 Self-defence and Self-regulation....170
5.8 Conclusion....172

6 Cyber-terrorism: An Emerging Security Risk 174
6.1 Introduction 174
6.2 Defining Cyber-terrorism 175
6.2.1 Critique of Denning’s Narrow Definition of Cyber-terrorism 177
6.2.2 Increasing Number of Cyber-attacks 179
6.3 The International Dimension 182
6.4 Cyber-terrorism Cooperation 183
6.5 Transnational Cooperation 185
6.5.1 The EU and External Cooperation 186
6.5.2 The EU and Internal Cooperation 189
6.6 Cross-sectoral Cooperation 190
6.6.1 The EU’s Public-Private Partnership 192
6.6.2 Governance Structures 193
6.7 Accountability, Transparency and Openness in the Anticipatory Governance Framework 195
6.7.1 Transparency and Openness and the Lack of Communication 196
6.7.2 Attracting Private Actors to the EP3R 197
6.7.3 The Visibility and Outcome of the Cooperation 197
6.8 Anticipatory Governance and the Development of Rules, Practices and Processes 199
6.8.1 State Regulation 200
6.8.2 Technical Regulation 201
6.8.3 Awareness-raising and Education 202
6.8.4 Self-defence and Self-regulation 204
6.9 Conclusion 205

7 The Understanding of Cyber-Security Governance and Practices in the European Region: The Concluding Chapter 208
7.1 The Research Objectives 208
7.2 The Contribution to Existing Knowledge 209
7.3 The European Challenge of Cyber-security 210
7.3.1 Anticipatory Governance 211
7.3.2 The Security Sectors 211
7.3.3 The Security Approaches 212
7.4 Conclusions and Normative Reflections 213
7.4.1 The Complexity of Cyber-security 216
7.4.2 The Governance Lacuna 217
7.4.3 Reliance on Different Governance Forms 218
7.4.4 Accountability and Transparency 219
7.4.5 Anticipatory Governance and Regulatory Practices 220
7.5 Future Research Areas 221
7.6 Final Remarks Regarding Future Research Areas 223

8 Bibliography 225

9 Appendix 264
9.1 Appendix 1: The European Region 264
9.2 Appendix 2: Research Keywords 265
9.3 Appendix 3: Chapter Five 266
9.4 Appendix 4: Statistic Data Regarding Cyber-crime 267
9.5 Appendix 5: Cyber-attacks 268
9.6 Appendix 6: Infrastructure 276
9.7 Appendix 7: EU Security Agencies 276
9.8 Appendix 8: Regulatory Framework 277

Figures and Tables

Figure 1 illustration of a DDoS attack....50
Figure 2 model for advancing the discussion 61
Figure 3 the security management process....86
Figure 4 resilience and preparedness in the risk-management circle 89
Figure 5 the continuous circular processes of risk-security management 92
Figure 6 the ongoing security governance circle 94
Figure 7 model for advancing the analytical framework....124
Figure 8 cyber-attacks (1999–2014) based on appendix3 181

Table 2. Primary research objective....17
Table 3. Specific research objectives 18
Table 4. Future research areas 223

Words: 80.957.

2 Abstract

This thesis explores the nature of cyber-security at the beginning of the 21st century. In the current security paradigm, security strategies based on anticipatory governance have become essential in the management of the constantly changing cyber-security environment. Thus, this thesis aims to understand security strategies and governance introduced in the European region. The increased dependency on cyber-space is visible in all public-private sectors and governmental operations, as well as communications between groups and individuals. As a result, cyber-attacks on public and private entities are increasing. This requires a security framework that is flexible and establishes different types of security cooperation to manage the widespread cyber-risks. This is essential to the development of security strategies, governance forms, practices, and guidelines for enhancing resilience and preparedness towards cyber-risks. Therefore, I am examining cyber-security through the lenses of nodal governance and governmentality, which enables me to understand European cyber-security strategies and governance forms developed by the Council of Europe, the European Union, and the North-Atlantic Treaty Organization. To analyse existing strategies and governance forms, I have used two critical security schools, the Copenhagen School and the Paris School, which cover different aspects of the security agenda. The thesis develops a substantive analytical framework through two case studies, namely cyber-security and cyber-terrorism. The findings in this thesis identifies problem areas, such as the complexity of the nodal system, the legislative lacuna, reliance on different governance forms, transparency and accountability, and types of anticipatory governance and regulatory practices.

Keywords: Anticipatory governance, awareness-raising and education, Council of Europe, cyber-attacks, cyber-crime, cyber-security, cyber-terrorism, Europe, European Union, governmentality, (in)security, NATO, nodal governance, risk, state-regulation, security, securitization, self-regulation and self-governance technical regulation, the Copenhagen School, the Paris School, threat, transnational and cross-sectoral cooperation.

3 Declaration

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

4 Copyright Statement

5 Acknowledgements

I could not have written this thesis without the help and support of a large number of exceptional people, who have challenged and supported me in my professional life as well as my personal life. I would like to express gratitude to my family and friends for their constant backing and understanding. Therefore, I have dedicated my work to family and friends, but I will refrain from mentioning all by name. Nevertheless, a handful of people deserve special thanks for their involvement, work and support.

The thesis is a result of a long process of interactions, discussions, corrections and exchanges of ideas with my two supervisors. Firstly, I would like to express my special appreciation and thanks to my supervisors Professor Dr. Toby Seddon and Professor Dr. Dora Kostakopoulou for encouraging my research and for allowing me to grow as an academic. My special thanks and acknowledgement goes to Professor Dr. Toby Seddon for his work and guidance in 2014/2015. I have had the best support I could have wished for throughout the writing of the thesis.

A special thanks goes to Dr. Graham Smith. He has been my unofficial mentor by constantly guiding and challenging me to come out of my comfort zone. I will also express my gratitude to Dr. Jasem Tarawneh for his support and advice, and finally to Dr. Betham Loftus, Dr. David Booton, Jackie Boardman, Kirsty Keywood, Dr. Mark Reiff, and Stephen Wadsworth, and everyone at the University of Manchester, who have supported me throughout this project.

I would also like to thank a handful of people who have always been there: ready to read, discuss, comment and correct different sections and chapters whenever I needed it. Thanks to Georgia Mouskou (Mouskou Mou), Inge Ankjær, Tine Lee Senft, Elsa Dufay and Christopher Markou. I also want to express thanks to Lee Wood for proofreading of the whole thesis. Your work made a significant difference. I also wish to thank Inge and Evald Munk, who were ‘forced’ to check the bibliography and footnotes. Finally, I will thank some special people, who have made my PhD time much more enjoyable and fun. You have constantly reminded me of the world outside academia. Thanks to Inge Ankjær and John Bertz, Elsa Dufay, Maibritt and Jan Falkesgaard, Ann Richter, Christopher Markou, Georgia Mouskou, Tine Senft, Dr Jasem Tarawneh, and my family: Inge and Evald Munk, Jesper and Laura H. Munk, and all the kids: Emma, Emil, and Jeppe H. Munk.

6 Abbreviation

Abbreviation	Full name
ASEAN	Association of Southeast Asian Nations
AU	The African Union
CERT	Computer Emergency Response Teams
CEU	Council of the European Union
CFSP	The Common Foreign and Security Policy
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CoE	The Council of Europe
DDoS	Distributed Denial of Service
DoS	Denial of Service
EC	European Commission
ECo	European Council
EC3	European Cybercrime Centre
EC/HREUFASP	The European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy
ECSC	The European Coal and Steel Community
EFMS	The European Forum of Member States
EISAS	The European Information Sharing and Alert System
ENISA	European Network and Information Security Agency
EP	European Parliament
EP3R	European Public-Private Partnership for Resilience
EU **Eurojust**	The European Union The European Union's Judicial Cooperation Unit
Europol	European Union's Law Enforcement Agency
G8	Group of Eight
ICTs **ITU**	Information and Computer Technologies The International Telecommunication Union
L.N.	The League of Nations
MERCOSUR	Mercado Común del Sur / Southern Common Market,
NATO	The North Atlantic Treaty Organization
NAFTA	North American Free Trade Agreement
NIS	Network and Information Security
OAS	Organisation of American States
OECD	The Organisation for Economic Co-operation and Development
OSCE	The Organization of Security and Cooperation in Europe
PPP	Public-Private Partnerships
SitCen	The Joint Situation Centre
UN	United Nations
WWI	World War One
WWII	World War Two

7 Glossary[1]

Botnet	Indicates a network of computers that have been infected by malicious software (computer virus). Such networks of compromised computers (‘zombies’) may be activated to perform specific actions, such as attacks against information systems. These ‘zombies’ can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This ‘controlling’ computer is also known as the ‘command-and-control centre’. The persons who control this centre are among the offenders, as they use the compromised computers to launch attacks against information systems. It is very difficult to trace the perpetrators, as the computers that make up the botnet and carry out the attack, might be located elsewhere than the offender himself.
Denial-of-Service (DoS) attack.	A denial of service attack is an act to make a computer resource (for example a website or Internet service) unavailable to its intended users. The contacted server or webpage will show itself as "unavailable" to its users. The result of such an attack could, for example, render online payment systems non-operational, causing losses for its users
Information System	Any device or group of interconnected or related devices, one or more of which, pursuant to a programme, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance. An example of this is a computer or a server.
Large-scale attacks	The either attacks that can be carried out by big botnets or attacks that cause considerable damage, e.g. in terms of disrupted system services, financial cost, loss of personal data, etc. The damage caused by the attack can have a major impact on the functioning of the target itself, and/or affect its working environment. In this context, a ‘big’ botnet will be understood to have the capacity to cause serious damage. It is difficult to define botnets in terms of size, but the biggest botnets witnessed were estimated to have between 40,000 to 100,000 connections (i.e. infected computers) per time span of 24 hours.
Malware	Computer software designed to infiltrate or damage a computer system without the owner's consent. It is distributed through a variety of means (emails, computer viruses and botnets). Intention is to obtain data (passwords, codes) in a fraudulent way, or to integrate this computer in a computer network destined to be used for criminal actions.

[1] EC (2010) ‘Proposal for a directive on attacks against information systems, repealing framework decision 2005/222/JHA’.

1 Introduction

1.1 Introduction

At the beginning of the millennium, government computer systems operated on dedicated networks, which were comparatively easier to protect. This is no longer the case. The highly decentralised and increasingly complex Internet is anchored in nearly every aspect of public and private computing. Mobile 'ubiquitous' computing has further complicated security efforts by multiplying the potential access and breach points. What now constitutes a cyber-security risk has evolved from being a simple matter of protecting a computer network from outside intrusions or physical access, to protecting entire nations, its citizens and their most sensitive information. For all of its user friendly attraction and promises, the Internet is effectively a 'series of tubes' and 'clouds' that connect everything from Facebook accounts, to bank accounts, to aspects of critical governmental and private infrastructure.[2]

Cyber-space creates a virtual world that enables criminal acts, where the

> "[C]riminal activity takes place within or by utilising networks of electronic communication such as the Internet".[3]

Barlow's Declaration of the Independence of Cyber Space (the Declaration) proclaims hackers as the owners and guardians of a free and independent cyber-space:

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature, and it grows itself through our collective actions".[4]

During the cyber-idealism period of the mid 1990s, and a few years before the dot-com bubble burst, the Declaration described hackers as curious youthful spirits. The

[2] Blum (2012) 'Tubes, a journey to the centre of the Internet'.

[3] Deibert and Rohozinski (2010b) 'Risking security: Policies and paradoxes of cyberspace security,15-16. Yar (2006) *Cyber-crime and society,*155.

[4] Barlow (1996) 'A declaration of the independence of cyberspace'.
Yar. (2006), 23. Wark (2006) 'Hackers'. Cf. Mitnick and Simon (2013) *Ghost in the wires.*

Declaration claimed that hackers should be celebrated, and have the right to access cyber-space freely, in order to exchange knowledge and information.[5] The Hacker's Manifesto states:

> "Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something you will never forgive me for".[6]

In the cyber-world, a hacker is considered to be someone who seeks knowledge for knowledge's sake, not because of the purity of his or her intentions. The 'black hat' hacker's aggressive way largely overshadows the naïve and curious 'white hats' ethical hacktivism.[7] The growing influence of cyber-space and the Internet in everyday life has created manifold opportunities for exploiting the weaknesses in the virtual world. Consequently, 'black hat' hackers have developed technologically advanced ways of searching computer networks for vulnerabilities and compromising individual and networks of computers.[8] The reality of cyber-space in the 21st century is that nothing is secure. Hackers have proven their capability to attack computer systems, and their resiliency to stay one-step ahead of security actors.[9] The updated Hacker's Manifesto 2.0 states:

> "Hackers create the possibility of new things entering the world. Not always great things, or even good things, but new things. In art, in science, in philosophy and culture, in any process of knowledge where data can be gathered, where information can be extracted from it, and where in that information new possibilities for the world produced, there are hackers hacking the new out of the old".[10]

The following outline shows that hackers are responsible for numerous cyber-security problems, and these problems continue to proliferate (appendix 5). Recent high-profile examples include the 2013 attack on the cryptocurrency, Bitcoin, which was plagued by hacks, Ponzi schemes,[11] increasingly professional cyber-thefts[12] and claims that it has

[5] Barlow (1996). Yar (2006),23. Wark (2006) 'Hackers'. Cf. Mitnick and Simon (2013).

[6] The Mentor (1986) *The conscience of a hacker (Hacker's Manifesto).* Wall (2007) *Cybercrime*,55.

[7] Cf. Barber (2001) 'Hacker' profiled'. Mansfield-Devine (2011) 'Hacktivism: Assessing the damage'.

[8] Jordan and Taylor (2004) *Hacktivism and cyberwars*,5. Yar (2006), 23. Everett (2009) 'Ethics – a question of right or wrong'.

[9] Jordan (2013) *Hacking: digital media and technological determinism*.

[10] Wark (2004) 'Hacker's manifest version 2.0.

[11] "*A Ponzi scheme is a scam investment designed to separate investors from their money Once the scam artist feels that enough money has been collected, he disappears - taking all the money with him".* Moffatt (2014) 'Ponzi scheme'. Hern (2013) 'A history of bitcoin hacks'.

[12] "*Stealing of financial and/or personal information through the use of computers for making its fraudulent or other illegal use".* BusinessDictionary (2014) 'Cyber theft'. Hern (2013) 'A history of bitcoin hacks'.

enabled other illicit trades such as drugs and child pornography.[13] During 2013, Facebook, Twitter and Apple were also hacked, with a significant number of their users' data and passwords stolen.[14] Adobe was also attacked during 2013, later confirming that personal details of 2.9 million customers had been stolen.[15] Apple's iCloud service, which allows Apple users to synchronise photos and other data came under scrutiny after intimate images of celebrities were stolen and leaked in 2014.[16] In 2014, a hack of eBay's user database resulted in the compromise of encrypted passwords and other non-financial data.[17] The Heartbleed bug in the OpenSSL cryptography library also caused problems in 2014. The bug allowed hackers to steal sensitive cryptographic keys protecting online commerce and web connections, and leaked personal data.[18] In 2014, Russian hackers attacked the American security company, Hold Security, and stole more than 1.2 billion usernames and passwords associated with more than 500 million email addresses.[19] However, the most high-profile attack was against Sony Pictures Entertainment towards the end of 2014. A hacking group, claiming the name Guardians of Peace, targeted the US based Japanese film studio and compromised extensive email 'spools', financial data, business plans, scripts, and several unreleased movies – especially the movie called 'The Interview', which portrays the assassination of the North-Korean leader Kim Jong-un.[20] In response to the attack, Sony Pictures temporarily delayed the film's release following a number of threats to the company.[21] The Sony attack provoked intense debate about cyber-security and cyber-attacks as a new dimension of warfare.

Attacks are not only fragmented criminal activities, but they constitute a growing illegal enterprise across territorial boundaries. Cyber-attacks have profoundly affected the economic and privacy interests of companies and their customers. However, this is only a cursory review of cyber-attacks, with many others going unannounced or undetected. The review also demonstrates that the challenge of cyber-security demands a greater understanding of network security, as well as an increase in international cooperation to

[13] Schweizer (2014) 'Bitcoin payments by pedophiles frustrate child porn fight'.
[14] BBC News (2013b) 'Apple moves to close Java hack flaw after intrusion'.
[15] BBC News (2013a) 'Adobe in source code and customer data security breach'.
[16] Miller (2014a) 'Apple iCloud security exploit is a concern, experts *say'*. Shontell (2014) 'Apple statement on celebrity hacking'.
[17] Kelion (2014a) 'eBay makes users change their passwords after hack'.
[18] Hern (2014) 'Heartbleed'.
[19] BBC News (2014b) 'Russia gang hacks 1.2 billion usernames and passwords'.
[20] Walker (2014) 'North Korea threatens US, claiming White House was involved in film plot'. BBC News (2014c) 'Sony hack'. Press Association (2014) 'Draft script for James Bond film Spectre leaked in Sony hack'.
[21] Walker (2014). BBC News (2014c).

address contemporary cyber challenges. The scope and complexity of the global internet infrastructure shows that no single actor can manage cyber-space. Although, this has not prevented some nations from attempting to 'Master the Internet'.[22] Alternative cooperative alliances must continue to be formed to maximise resilience to cyber-attacks worldwide. Despite numerous initiatives to bring down the criminal cyber-activities, destroying one network often results in the establishment of another, forcing hackers to innovate upon their methods, and in turn, allow new cyber-risks to develop. Nonetheless, the frequency of attacks demonstrates the need for new security directions, guidelines and practices to counter cyber-risks worldwide. The central complication of this task is that the virtual world is extra-territorial, with no fixed boundaries applying to legal or illegal online activities in the same way as the rules and regulations developed in the real world.[23] This gives creative hackers the opportunity and freedom to obtain control over interconnected.[24]

Cyber-security and cyber-space are abstract areas. It is possible to define and describe visible areas and patterns. However, it is impossible to get a full picture because the future is unpredictable, and the scientific journey into a digital universe with unlimited opportunities has only just begun. Only our imagination and technical skills are boundaries, and at this point, our understanding of its potential is limited. I believe that it is possible to identify processes, structures, opportunities, and dangers, and we can to some extent predict and estimate how future computer science and technologies will influence us by using existing knowledge. Nonetheless, the growing number of cyber-attacks puts greater pressure on security actors to increase security in order to manage eventualities.

Policy-makers and academics needs to pool resources to understand the new security structure and the parameters of the future-oriented cyber-security concept, i.e. by enhancing resilience building, prevention and preparedness. These anticipatory measures are included in the collection of policies, practices, and technologies designed to protect the cyber environment, its organisation and users' assets.[25] As a result, the global community, security experts, etc. face profound challenges in rethinking security and making changes to policy. Intellectually, it is important to address the way

[22] MacAskill et al (2013b) 'Mastering the Internet'.
[23] Strate (1999) 'The varieties of cyberspace'
[24] Avina (2011) 'Public-private partnerships in the fight against crime',286.
[25] ITU (2014) 'Cyber security definition'.

academics think about the cyber-security risks and the organisation of security actors as there is no global organisation through which information passes.[26] Instead, security governance and information sharing are distributed across numerous independent trajectories within a network.[27]

1.2 The Research Objectives

Cyber-security, the capacity of networked computer technologies and the related socio-political challenges they present are some of the central issues of the 21st century. The technological development shows the imminence of new security challenges which security actors are unprepared for at governance and operational levels. The primary governance issue is the organisation of cyber-security strategies that now include state and non-state actors in a multi-levelled framework that circumvents state-centric management. The recent high-profile cyber-security issues that have been highlighted above have been influential in allowing both policy-makers and the public to accept that cyber-related crime is an increasingly serious problem, with potentially catastrophic, political, economic and social implications. The Sony Pictures attack has been the catalyst for a marked shift in governmental and public concern over the efficient management of cyber-risks and the need for increased cooperation between actors. However, the challenges of cyber-security, together with the troubled alliance between state and private sector actors, create additional tensions for security and technology policy problems. These problems require further attention, and it is the aim of this thesis to examine and investigate them. In this thesis, cyber-security is examined within the European framework, with a particular emphasis on anticipatory governance practices.

The primary research objective of this thesis is to critically examine an area of cyber-security governance which has been overlooked in the academic literature and ineffectively managed by governments. The existing literature focuses on diverse areas of cyber-security, such as U.S. governance and management methods,[28] the Council of Europe's Convention on Cyber-crime,[29] international cooperation, critical infrastructure (CI), critical information infrastructure (CII), and information computer technologies

[26] Deibert (2002) 'Circuits of power, security in the Internet environment',132.

[27] Dam and Lin (1996) *Cryptography's Role in Securing the Information Society*,22, 27.

[28] Cf. Arquilla and Ronfelt (1999) *The emergence of noopolitik*. Brunner, and Dunn Cavelty (2009) 'The formation of in-formation by the US military'. Clarke (1999) 'Threats to US national security'. Clarke and Knake (2011) *Cyber war*. Bendrath et al (2007) 'From'cyberterrorism'to'cyberwar'. Bendrath (2001) 'The cyberwar debate'. Brito and Watkins (2011) 'Loving the cyber bomb'. Lawson (2012) 'Putting the "war" in cyberwar'.

[29] Cf. Keyse (2002) 'The Council of Europe Convention on Cybercrime'. Moore et al (2009) 'The economics of online crime'. Levi and Wall (2004) 'Technologies, security, and privacy in the Post-9/11 European information society'. Broadhurst (2006) 'Developments in the global law enforcement of cyber-crime'.

(ICTs), and specific cyber-crime areas like privacy, policing, surveillance, data protection, cyber-law and social media.[30] To answer the research objective, this project explores nodal governance structures that include both transnational and cross-sectoral cooperation in cyber-security. The nodal governance framework requires security actors to form alliances beyond their traditional security partners on order to advance governance forms. The overall research question, in combination with the sub-objectives, enables this project to adopt a novel approach to discussing cyber-security, differentiated networks of security actors, multi-levelled cooperation strategies, and anticipatory governance forms on the strategic level. This research project attempts to provide a more nuanced understanding of cyber-security governance and trends, such as the shift away from the normative state-centric security policies.

Primary objective
To examine contemporary European cyber-security strategies and their governance forms

Table 1 primary research objective

This thesis adopts nodal governance as the organisational foundation for understanding and addressing the challenges of an interconnected system, which is a dynamic and ongoing process. Anticipatory governance practices are developed on multiple levels in a hybrid-networked formation, where security actors selectively cooperate on a case-by-case basis. I argue that cyber-security governance and practices reveal a more complex structure, which requires alternative methods for ensuring meaningful security. The Declaration of the Independence of Cyber Space and the Hackers Manifesto states that traditional boundaries, sovereignty and power structures have broken down and they are being replaced by a new distribution of knowledge and power.[31] The justification for using this research question is that cyber-security governance is overlooked in academia, which is surprising as the strategies establish a conceptual framework and the direction of security responses in a networked security formation. Furthermore, the role of both the private sector and individuals in cyber-security is also mainly ignored in

[30] CF. Svantesson and Clarke (2010) 'Privacy and consumer risks in cloud computing'. Weber (2010) 'Internet of things'. Schermer. (2011) 'The limits of privacy in automated profiling and data mining'. King and Raja (2012) 'Protecting the privacy and security of sensitive customer data in the cloud'. Wong (2011) 'Data protection'. Hiller and Russell (2013) 'The challenge and imperative of private sector cybersecurity'. Aquilina (2010) 'Public security versus privacy in technology law'. Bauman et al (2014) 'After Snowden'.

[31] Barlow (1996). The Mentor (1986). Wark (2004).

cyber-security discussions. The rationale for including both areas, are as follows: Firstly, both state and non-state actors are at risk of being attacked. Secondly, different groups of actors have experience with developing preventive governance and management forms.

The primarily objective of this thesis is advanced using two secondary objectives, which cover specific areas of the research.

	Secondary objectives
1	To evaluate the adequacy of existing governance forms, concepts of risk, and security approaches and perspectives for understanding cyber-security problems
2	To examine whether European policies and strategies for dealing with emerging security risks, i.e. cyber-security and cyber-terrorism, generate new insights into thinking about risk and security in the twenty-first century

Table 2 specific research objectives

The two secondary objectives are guidelines for answering the primary objective. The first secondary objective is linked to the first part of the thesis, and assists in the investigation of governance forms, risk and relevant security approaches. The primary objective is addressed through a literature review of different definitions, governance forms and security schools. Before beginning any discussion on cyber-security, it is important to understand the interplay between cyber-security and the capacity of networked computer technologies, and the related socio-political challenges. Therefore, the first specific research objective is to analyse the existing security framework, security approaches, and the concept of risk, to establish a theoretical and substantive understanding of this area. The rationale for including this analysis in the framework is that current cyber-security research does not cover this area, thus creating lacunae in understanding how cyber-security is conducted and whether it is adequate to respond to the cyber-risks in the current security environment. The literature review includes concepts and definitions necessary to understand cyber-security and the critical security perspectives of this thesis. To analyse this area, the approaches of two established security schools, the Copenhagen School of Peace and Conflict (the Copenhagen

School) and the Paris School on Security (the Paris School), are examined to utilise the cyber-security discussion, explore conceptual matters and to sharpen and critique the existing framework.

The second secondary research objective follows on from the first objective, allowing an insight into the related topics of cyber-security and cyber-terrorism. So far, only limited aspects of these two cyber-security areas have been investigated in academic literature, despite expectations that cyber-security and cyber-terrorism will rapidly expand in light of continued technological innovation and its attendant social complications. The rationale for this approach is that, even though these two cyber-concerns are recognised worldwide, they remain under-researched in relation to anticipatory cyber-governance in the European context. The first case study investigates a number of leading European organisations' cyber-framework developed to manage the overarching concept of cyber-security. The second case study covers cyber-terrorism, which is an issue high on the global security agenda, where it has been identified as a significant and increasing risk. Cyber-terrorism research is limited and often overlaps with cyber-crime and cyber-warfare issues. By separating cyber-terrorism from the other two sub-units, I offer an in-depth analysis of an under-research area. Therefore, this research project develops a novel approach to understanding anticipatory governance of cyber-terrorism.

1.3 Aim and Scope of the Research: The Contribution to Existing Literature

The aim of this project is to offer a greater insight into the different forms of cyber-security governance. I will analyse anticipatory governance and practices in the European region, which are determined by the geographical position and cooperative regionalism considered from their involvement in three European security institutions – North-Atlantic Treaty Organization (NATO), The Council of Europe (CoE), and the European Union (the EU) (appendix 1). The EU has developed a comprehensive security structure incorporating numerous cyber-security concerns, actors and agencies, as well as cooperation forms and legislation. As a result, I have drafted most of the research on this regional security institution's initiatives. In cyber-security, an active cooperative structure is required as these unlawful activities are not limited to one jurisdiction alone. This perspective broadens the security agenda by requiring a horizontal and vertical approach involving public and private sectors, groups and individuals.[32] Rothschild has described security interactions between sectors and actors as:

> "[D]iffused in all directions from national states, including upwards to international institutions, downwards to regional or local governments, and sideways to non-governmental organisations, to public opinion and the press, to abstract forces of nature or of the market. The geometry…. is… of dizzying complexity".[33]

This citation captures the core element of this thesis. Security governance and practices are defined by the complexity that blurs the overview of the hybrid networks structure, the different actors and the organisation of security responses. Nevertheless, the nature of cyber-risk requires a broadly formulated approach where the security actors attempt to cover as many potential risk areas as possible. The aim of this approach is to understand European cyber-security strategies and their governance forms, which will involves looking at existing definitions, concepts and governance forms in order to obtain knowledge about a growing security concern.

The scope of this thesis and my contribution to the existing knowledge and literature is linked to five different areas. These areas are discussed throughout the thesis. Firstly, I include the European region. I have focused on this region, because it has been an area in which several significant conflicts have occurred in the last century (appendix 1). As a result, several security agencies and institutions have been established to prevent future conflicts and security concerns, and Europe has been at the forefront of the cyber-development in the last decade. This prime position has resulted in the introduction of a significant number of cyber-security strategies, road maps, and action plans to manage the growing number of cyber-risks, which are useful for my analysis. Another reason to include the European region is that the development of cyber-security responses are more established in Europe compared with other regions – and these responses continue to develop at a fast pace. In this context, the governance forms are primarily based on cooperation and hybrid networks created to increase resilience in the area. Despite the great potential of using Europe as a case study, I have not been able to find any scholars who have used it for this purpose, apart from when carrying out an analysis of specific issues, institutions or legislation, such as the Council of Europe's Convention on Cyber-crime, NATO, and fragmented areas of the EU. I find it interesting that European cyber-security strategies are left out of academic research.

[32] Zedner (2009) *Security*,13.
[33] Zedner (2009),49. Rothschild (1995) 'What is security?',55.

Secondly, the foundation of the study is anchored in nodal governance, which derives from the work of Shearing, Burris, Johnson, Wood and Dupont. As a result of using the nodal foundation, this thesis will differ from other cyber-security studies because it will bring the work of Shearing et al into the internet age.[34] The way in which Shearing et al understanding security is compatible with the extended use of hybrid networks in cyber-security, where governmentality plays a significant role in framing and analysing security responses. Nevertheless, this area is already thoroughly investigated by scholars such as Dean, Rose, O'Malley, Valverde, Garland, etc. The research conducted by these scholars is primarily based on a conceptual discussion or in combination with the concept of risk, where I narrow down the discussion to cover anticipatory governance and practices.[35] Discussions on threat and threat-based policies have been monopolising security discourse for decades. The result of using the concept of risk as the primary focus allows me to set these threat-based policies aside. Instead, I concentrate on the uncertainty and the high probability of cyber-risks in relation to cyber-governance.

The concept of risk is critically reviewed in security literature, and technologies of risk-management deployed for the purposes of security governance are well established. Consequently, prominent security scholars influence the progression of the risk-based analysis in this thesis, i.e. Beck, Luhmann, Ewald, whereas McCulloch and Pickering, Amoore and de Goede, Walklate and Mythen, O'Malley, Garland, Aradau and van Munster, etc., contribute significantly to the literature reviewed in part one of this thesis.[36] A large number of security studies are based on counter-terrorism measures, practices and governance forms, which have occupied security studies significantly since 9/11. This thesis has a different scope because I have chosen to link the discussion to emerging security issues which are surfacing in a socio-technology environment because of the increased reliance on computer technologies. This signifies that 'good' technological development can quickly embrace the 'bads' in a paradoxical

[34] Wood and Shearing (2007) *Imaging security*,21. Burris et al (2008) 'Changes in governance'. Burris et al (2005) *'Nodal Governance'.*

[35]Dean (1999) 'Risk, calculable and incalculable'. Dean, (2002) 'Powers of life and death beyond governmentality',138. Rose et al (2006) 'Governmentality'. O'Malley (2009) 'Governmentality and risk'. Garland (1997) ''Governmentality' and the problem of crime'.

[36] Luhmann (1993) 'Risk: A sociological theory', Ericson and Doyle (2004) 'Catastrophe risk, insurance and terrorism'. McCulloch and Pickering (2009) 'Pre-Crime and counter-terrorism'. O'Malley (2009). O'Malley (2012) 'Security after risk'. Aradau and van Munster (2007) 'Governing through risk'. Aradau and van Munster (2008) 'Taming the future'. Garland (2003) 'The rise of risk'. Beck (1992) The risk society'. Beck (1994) 'The reinvention of politics'. Beck (2002) 'The terrorist threat'. Mythen (2004) *Ulrich Beck.* Amoore and de Goede (2008b) '*Risk and the War on Terror*. Amoore and De Goede (2005) 'Governance, risk and dataveillance in the war on terror'. De Goede (2008a) 'Beyond risk'. De Goede (2008b) 'The politics of preemption and the war on terror in Europe'.

relationship.[37] These 'bads' constitute a severe risk, and the responses to them are developed from a future-oriented perspective where security actors develop anticipatory measures and governance forms to manage the potential cyber-risks.

Thirdly, I have chosen to include anticipatory governance to the security framework. The growing focus on risk in everyday life requires security actors to manage cyber-risks in order to increase resilience and decrease vulnerability through governance forms. Critical security scholars, such as O'Malley, Rose and Lentzos, Wakelate and Mythen, Aradau and Van Munster incorporate imaginative scenarios, resilience and preparedness in their research.[38] In this thesis, I have linked the critical risk literature together with literature addressing governance and practices of anticipation, such as resilience, preparedness, precaution and pre-emption.[39] As a result, I believe that the concepts of resilience and risk are interlocked in a complex structure that has emergent qualities that infuse the security environment with uncertainty.[40] Nevertheless, none of these scholars applies the concept of resilience and preparedness to the virtual world by merging the social and technological development with the proactive security approach. In this thesis, I have focused my analysis on anticipatory governance and practices introduced to enhance the resilience in society by targeting vulnerabilities in CI, CII and ICTs. These vulnerabilities are arising from the rapid socio-technological development and the growing reliance on cyber-space in everyday life (chapters 3 and 4). In practice, this means the governance structures enable security actors to develop different forms of rules, regulation and practices, i.e. through transnational and cross-sectoral cooperation (chapter 5 and 6). My own understanding of cyber-security mirrors the constant changes in cyber-space, computer technologies and electronic communication. Therefore, the concept advances in synergy with the anticipatory approach. This has also been the catalyst in other fields of science, where the socio-technological development is vital. I have chosen to include the anticipatory governance similar to other emerging areas, such as nanotechnology, computing, climate change and synthetic biology.[41]

[37] Beck (1992).

[38] O'Malley (2012). Lentzos and Rose (2009) 'Governing insecurity'. Aradau and van Munster (2008). Aradau and van Munster (2007). Walklate et al (2013) 'Searching for resilience',15. Walklate et al (2013b) 'States of resilience and the resilient state,12.

[39] Dunn Cavelty et al (2015) 'Resilience and (in)security',6. Adey and Anderson (2012) 'Anticipating emergencies', Aradau and van Munster (2012) 'Politics of Catastrophe'. Petersen (2012) 'Risk analysis'.

[40] Dunn Cavelty et al (2015), 6

[41] *Guston, for example, has done significant work in relation to explaining anticipatory governance structures of nano-technology, which shares significant parameters with cyber-security*. Guston (2014) 'Understanding 'anticipatory governance'. Cf. Barben et al. (2008) 'Anticipatory governance of nanotechnology'. Anderson (2007)

Fourthly, I will focus on cyber-security and its application in a broader context. In doing so I will not just limit my focus to the concept of cyber-crime, which will distinguish this thesis from a number of socio-legal studies in this field. Academics such as Denning, Wall, Yar, Deibert and Rohozinski, Arquilla and Ronfelt, and Dunn Cavelty have done pioneering research to enhance the understanding of cyber-security.[42] However, a remarkable gap in the literature remains by ignoring European risk-based security strategies and anticipatory governance and practices. Cyber-security and its sub-categories of cyber-crime, cyber-warfare and cyber-terrorism are mostly interpreted from a general perspective, or from the viewpoint of the United States (the U.S.), the national state or by using a particular area of the concept. My contribution to the existing literature derives from two case studies where I investigate European cyber-governance forms and practices, i.e. cyber-security and cyber-terrorism. In the first case study, I investigate cyber-security based on a broad governance discussion, which sets out an overall framework for managing cyber-risks in Europe. In the second case study, I narrow down the research to one particular security sub-category under the cyber-security umbrella, where I investigate the emerging concept of cyber-terrorism. This particular area of research lacks a clear definition and as a result, the concept is partly divided into counter-terrorism and cyber-crime regulation. Additionally, cyber-terrorism has previously been neglected in academic literature, with most studies focusing on the two sub-concepts of cyber-security, i.e. cyber-crime and cyber-warfare.

Fifthly in this thesis, I use two well-known security approaches which have emerged from the Cold War, i.e. the Copenhagen and the Paris Schools. These critical security perspectives are essential for understanding the structures of the emerging cyber-risks and the features embedded in security actors responses. By outlining these security concepts, I am able to examine the depth and the breadth of European cyber-security strategies necessary for the execution of anticipatory governance forms. Dunn Cavelty

'Hope for nanotechnology'. Quay (2010) 'Anticipatory governance'. Karinen and Guston (2010) 'Toward anticipatory governance' Ozdemir (2009) 'What to do when the risk environment is rapidly shifting and heterogeneous?'. Gorman (2012) 'A framework for anticipatory governance and adaptive management of synthetic biology'.

[42]Cf. Denning (2006) 'A view of cyberterrorism five years later'. Denning (2010) 'Terror's web' Denning (2012) 'Stuxnet: What has changed?'. Wall (2010) 'The Internet as a conduit for criminal activity'. Wall (1998) 'Catching Cybercriminals'. Wall (2003). *Crime and the Internet*. Wall (2007). Yar (2013) *Cybercrime and society*. Yar (2005b) 'The novelty of 'cybercrime'. Yar (2005a) 'Computer hacking'. Deibert and Rohozinski (2010a) 'Liberation vs. control'. Deibert and Rohozinski (2008) 'Good for liberty, bad for security?'. Deibert and Rohozinski (2010b). Arquilla and Ronfeldt. (2001) *Networks and netwars*. Arquilla and Ronfeldt (1993) 'Cyberwar is coming!'. Dunn Cavelty (2007) *Cyber-security and threat politics*. Dunn Cavelty (2008) 'Cyber-terror—Looming threat or Phantom Menace?'. Dunn, Cavelty and Mauer. (2009) 'Postmodern intelligence'.

has used both approaches, but her application was linked to U.S. cyber-management.[43] I acknowledge that the two schools are critical approaches focusing on the analysis of governance and practices by exploring their political effect. The two security approaches generate insights and clarify the use of anticipatory governance. Although the securitization (Copenhagen) and the management of unease (Paris) are deployed to understand cyber-security, there is a lack of research concerning an in-depth analysis of the practices of governing cyber-security in Europe. Therefore, this unexplored area is included in this thesis. This thesis tweaks the Paris School's perspective and gives it a new foundation for understanding cyber-security on the strategic level. In relation to the Copenhagen School, I look into a new interpretation of the Copenhagen School's securitization by Nissenbaum and Hansen.[44] This theoretical perspective appears to be a work-in-progress. Nevertheless, it gives a new dynamic to the discussion, and I chose to use this new understanding of securitization to utilise cyber-security.[45]

1.4 Methodology

This thesis is based on qualitative research where I have analysed data from a variety of sources. The identified research objectives require a qualitative - rather than quantitative - approach as I have examined cyber-security based on a documentary analysis where I reviewed relevant academic literature in order to advance the theoretical cyber-security framework in the case studies (section 4.9). This is an interdisciplinary research project, where I have used sources from different research areas regardless of their scientific origin, and I have conducted interdisciplinary research where the theoretical basis spans different academic fields, such as political, sociological and legal insights. In order to identify, select, discuss and conclude on data found in the documentary research, I have used a mixture of a top-down approach and a grounded approach. This section outlines the underpinning research methodology by explaining how I have answered my research objectives. This is followed by two sections which narrow down the research areas. Firstly, the overall research area is described in section 3.2 and this is illustrated by figure 2. This area outlined the research area for the first part of the thesis. Secondly, section 4.8 synthesises the theoretical and the substantive parts of the thesis and this is illustrated by figure 7. However, it is also important to read this section together with

[43] Dunn Cavelty (2007). Dunn Cavelty (2008). Dunn Cavelty and Kristensen (2008) '{Securing\'the homeland\': critical infrastructure, risk and (in) security'. Brunner and Dunn Cavelty (2009).

[44] Hansen and Nissenbaum (2009) 'Digital disaster, cyber security and the Copenhagen School'.

[45] Hansen and Nissenbaum (2009).

the case-study methodology in section 4.9, because this section contains a more detailed explanation of the methodology used.

In this documentary analysis, I have analysed documents from within the framework of the two security perspectives, i.e. The Copenhagen School and the Paris School (chapter 4). While I do not adhere to a particular security perspective or school, I have drawn upon two perspectives to understand security in order to delineate my own approach. This study only involves the principles of the two security schools to investigate the core elements of cooperation and governance.[46] In doing so, I have limited the scope of the security study by leaving out other influential security perspectives, such as critical security studies, military/strategic studies, peace theory, feminist security studies, human security, etc.[47] Although these perspectives are influential and useful theoretical security perspectives, they are less compatible with the aim and the scope of this thesis.

I have used the Copenhagen School and the Paris School to criticise and sharpen the understanding of cyber-security structures because I want to utilise the parameters and the limitations of current governance forms. These two security schools offer a particular stance on security, which allows me to cover two different sides of the debate on cyber-security and governance (chapter 4). Both the Copenhagen School and the Paris School are critical approaches and both schools are related to security-discourses. Their critical perspectives on how security is managed make them relevant to include in the analysis of the complex cyber-governance area. In this context, I have focused on the history of discourse, information regarding the development, all its interrelations and transformations in relation to cooperation and nodal governance, and the critical approach of the two security schools. In the documentary analysis, I have included the two schools and their critical understanding of security to discuss the processes of discourse, the thresholds, which have led to a different perception of security, cooperation and the actors involved in the process. This framework enables me to analyse governance by differentiating between rationalities and the technologies of

[46] Buzan et al (1998) ‘Security. A New Framework for Analysis’. C.A.S.E. Collective (2006) ‘Critical Approaches to Security in Europe’,457.

[47] Cf. Booth (2011) ‘Critical security studies’. Buzan (1987) *An introduction to strategic Studies*. Betts (1997) ‘Should strategic studies survive?’. Grissom (2006) ‘The future of military innovation studies’. Rasler and Thompson (2005) *Puzzles of the democratic peace*. Conteh-Morgan (2005) ‘Peacebuilding and human security’. Paris and Sisk (2009) *The dilemmas of statebuilding*. Kaldor (2013). *Human security*. Roberts (2006) ‘Review essay: Human security or human insecurity?’. Wibben (2010) *Feminist security studies: a narrative approach*. Cohn (2011) ‘Feminist security studies’.

government, cyber discourses and the practices of different realities and heterogeneous strategies.[48]

This documentary analysis has enabled me to examine a large number of documents and it provides me with particular lenses for understanding and developing the research guided by the research objectives. I found this analytical concept useful for discussing cooperation, security actors and the complexity of cyber-security governance. From this perspective, I have adopted a constructivist analytical stance because it is impossible to predict the future, and therefore it is necessary to construct the security issue based on an objective and subjective perception.[49] In this thesis, cyber-security develops from a political and social construction, where social and technological developments are imagined to manage the techno-scientific cyber-risks. This stance has allowed me to acknowledge the subjectivity and my involvement in the construction and interpretation of the data.[50] Chapter 4 provides a more comprehensive outline of the methodology, where I have synthesised the research by connecting the theoretical foundation and the substantive analysis. Strauss and Corbin have developed the grounded theory around the use of particular research techniques, and these are applied in this section (section 4.9).[51]

The thesis is based on empirical research, where I have combined a top-down approach and grounded approach (chapter 4).[52] This indicates that I have not carried out an objective selection of knowledge by hoovering up the entire cyber-security field, and consummated it before highlighting the different rationales involved in this necessary to progress this research. Instead, my research and understanding of cyber-security derives from a selection process. In this process, I have established the research area based on a top-down research approach using the keywords in section 4.9. These keywords are useful for narrowing down the research and to outline relevant discussion areas.[53] Secondly, I have used a grounded approach, because I did not begin the research with a hypothesis but took a range of data sources, analysed them using a range of qualitative

[48] Foucault (2009),115-134. Lemke (2000),7.

[49] Healy and Perry (2000) ‘Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm’,119-120. Guba and Lincoln (1994) ‘Competing paradigms in qualitative research’,112.

[50] Charmaz (2014) ‘Constructing grounded theory’,13.

[51]Cf. Strauss and Corbin (1990) *Basics of qualitative research: Grounded theory procedures and techniques.* Corbin and Strauss (1990) ‘Grounded theory research: Procedures, canons, and evaluative criteria’. Corbin and Strauss (2014) *Basics of qualitative research: Techniques and procedures for developing grounded theor*y.

[52] Sabatier (1986) ‘Top-down and bottom-up approaches to implementation research’,23. Cf. Matland (1995) ‘Synthesizing the implementation literature’.

[53] Sabatier (1986).

methods and grounded my understanding of the problem in my observations (section 4.9).

Cyber-security is an emerging area, and traditional sources are not up to date with the constant technological changes, and this forces me to include other alternative sources for my data collection (section 4.9). Thus, I needed to collect a broad range of alternative material which shed light on questions under study.[54] Grounded theory is based on a systematic and flexible form of collection and analysis of qualitative data, and this method allows me to seek out patterns and structures of European cyber-security strategies.[55] I have grounded the data collection and analysis by using material from institutional documents, legislation, books, journal articles, reports, newspapers and web-pages (section 4.9). By carrying out the procedure of data collection and analysis systematically within the already established framework, I am able to proceed to capture all potentially relevant aspects of the topics as soon as they are perceived.[56] This signifies that the research strategy is not a linear process. Instead, it is an ongoing selection-process, where I have identified research areas, selected sources, and assessed and analysed the material to determine the relevance for this study and to develop a critical understanding of cyber-security and governance. The inclusion of a variety of data generates an initial understanding of European anticipatory risk-policies, which is useful for analysing and concluding on the findings.

This thesis consists of two parts, using two different perspectives, i.e. literature review and case study. In the first part of my thesis, I have carried out a literature review to establish the theoretical foundation of cyber-security. I made a systematic review based on the research objectives in order to progress arguments relevant to the thesis.[57] I have used the literature review to reinterpret existing publications, which are relevant to my two case studies. As a result, I have included materials from different sources in order to explore possibilities, rather than follow a strict and defined investigation.[58] To do so, I have reviewed a number of data to understand the concept of cyber-security, i.e. cyber-space, threat and security, nodal governance, risk, anticipatory governance. The first case study is related to European cyber-security and the second is related to cyber-

[54] Corbin and Strauss (1990) 'Grounded theory research: Procedures, canons, and evaluative criteria',5. Cf. Strauss (1987) *Qualitative analysis for social scientists*. Corbin and Strauss (1990) *Basics of grounded theory methods*.
[55] Corbin and Strauss (1990),5-7.
[56] Corbin and Strauss (1990),6.
[57] Cf. Creswell (2007) 'Review of the literature'. Hart (1998) *Doing a literature review*.
[58] Humphreys (2010) 'The heuristic application of explanatory theories in International Relations',262.

terrorism. I have specifically chosen these areas because they are strategically important, and I have used the two case studies to carry out an in-depth and detailed examination of cyber-security and its related conditions.[59] This approach highlights a particular way in which discourses engage with the present understanding of cyber-security by explaining how security methods and practices have developed. My strategy for analysing the documentary material aligns with the theoretical approach I have adopted. The key areas I was looking for in data were the same which the theoretical framework suggested were important (section 4.9).

1.5 Structure of the Thesis

Cyber-security strategies reveal a new security direction, which I will critically investigate throughout the analysis of anticipatory governance introduced in the European security framework. I have divided the thesis into two parts. Chapters 2, 3 and 4 will create the theoretical foundation based on a literature review in order to conceptualise security theories, approaches and concepts. In the first part of my thesis, chapter 2 defines threat and security and outlines the historical development of security processes and cooperation since World War I up to the recent security paradigm. This chapter also introduces the concept of cyber-security, which creates the foundation for discussing cooperation, risk and anticipatory governance. Chapter 3 is essential to the framework by theorising the overarching perspective of this thesis as nodal governance by utilising the understanding of governance forms and practices and the use of multi-actors. The concept of risk and its usefulness enables me to progress the cyber-security analysis, because I position anticipatory governance central to this thesis. As a result, my conceptualisation of cyber risk-management and governance includes resilience, preparedness and preventive tools, which all have a significant place in the ongoing security circle (figure 6). Chapter 4 defines and analyses two critical security schools developed in the aftermath of the Cold War. Both the Copenhagen and Paris Schools are critical to any study of security, and I have included them both because they are significantly influential in many areas of the security spectrum. In this thesis, they are fundamental to improving the empirical examination of cyber-security in chapters 5 and 6. The final part of chapter 4 connects the two parts of my thesis and explains the methodology used in part two. In this part, I have discussed the core elements of the substantial analysis, i.e. cooperation, security actors and the development of

[59] Mills et al (2010) *Encyclopaedia of Case Study Research*,xxxi. Yin (2014) *Case Study Research*,5-6.

anticipatory governance and practices. Moreover, in section 4.9 I have outlined the methodology for the case studies.

To progress the discussion, chapters 5 and 6 constitute the substantive analysis of the two case studies I have used to investigate the use of anticipatory governance in current cyber-security strategies. Chapter 5 advances the overarching concept of cyber-security and anticipatory governance. The discussion follows the outline made in the previous chapter regarding cyber-security governance and cooperation on different levels. The last part of the study is divided into sub-sections. These sub-sections will include state governance, technical governance, awareness-raising and education, self-defence and self-governance. Chapter 6 covers cyber-terrorism, which is an emerging area within cyber-security. The structure of the analysis follows chapter 5 and focuses on the protection of CI, CII and ICTs, where different forms of cooperation and governance are integral parts of the discussion. This chapter focuses significantly on the EU response, and includes the development of Public-Private Partnerships (PPPs), which have emerged as an alternative to the transnational structure. Finally, the last chapter sums up the analytical framework developed in this thesis. I conclude the analysis by outlining the original contributions and discuss the findings from the case studies.

PART ONE: THE THEORETICAL FOUNDATION OF ANTICIPATORY CYBER-SECURITY

2 The Evaluation of Security; From Threat to Risk

2.1 Introduction

Cyber-security is considered a growing political, economic and social threat, which is constantly evolving and challenging high-tech users globally. The way in which security is understood has developed rapidly over the last century, and this has had an influence on the recent risk-based security paradigm. In this thesis, the focus is on Europe, defined by its geographical, cultural or historical criteria (appendix 1). The contemporary understanding of European security is a direct consequence of wars and conflicts in the last century. Over the years, territorial war and conflicts have changed the security landscape beyond the military approach, and security has progressed from being a pure defence mechanism to becoming a broader concept, including non-military security problems.[60] However, threat is not a static concept, and the definition cannot be fixed to one particular end. Instead, it is important to link the understanding of both threat and security to a particular time and place because the two concepts differ between persons, situations, conditions and times. I have set out the foundation for understanding cyber-security by going back in time to observe which parameters have been significant and how they have developed over time. This enabled me to understand the way in which cyber-security is seen and governed, and it has been the underpinning foundation for progressing the research objectives outlined in chapter one.

This chapter is introductory to the whole thesis, and it frames the concept of security to enhance the understanding of the growing awareness of cyber-security and anticipatory governance through an analysis of the conceptual development of security. In this chapter, I outline key security dimensions to establish the discussion regarding the structural design and dynamics of cyber-security risks. I focus on how security and cooperation have changed over the years by anchoring the historical outline of Foucault's work on the archaeology of knowledge (section 1.4).[61] I analyse the historical development of security from WWI until the present time. This analytical foundation is based on how particular security strategies and measures can generate an

[60] Terriff et al. (1999) *Security studies today*,20.

[61] Foucault (1969).

understanding of the concept of cyber-security, its application, and the actors involved. Additionally, I outline core elements included in the concept of cyber-security.

2.2 Conceptualising the Relationship between Threat and Security

During the Cold War, threats were defined militarily from external sources. As a result, threats activated a defence mechanism to protect the sovereign state. In this hostile environment, new directions in security studies slowly began to emerge, including non-military security issues.[62] In this thesis, I frame the concepts, and position them in the correct historical period and geographical place in order to discuss the latest threat emerging because of technological development. Anticipatory governance forms have advanced in the risk-based security framework compared with traditional threat-based security. Nevertheless, I dedicate time to outline the concept and the historical development in terms of cooperation, institutions, and governance and practices. The underpinning concept is still prevalent as a secondary management form to catch unnoticed dangers if they transform into actual threats (chapter 3).

The definition of threat and security has changed over the years, and I consider the definition made by Ullman in the 1980s to be highly topical because of the way in which cyber-security is framed and governed. His work was pioneering because of his expansive interpretation of security that provided a broader understanding of threats at a time when military defence was seen as the only way to enhance security. He stated:

> “[A]n action or sequence of events that (1) threatens drastically and over a relative brief span of time to degrade the quality of life for the inhabitants of a state, or (2) threatens significantly to narrow the range of policy choices available to the government of a state, or to private, nongovernmental entities (persons, groups, corporations) within the state”.[63]

This is a very comprehensive definition, and it is still functional in the current security climate because it defines a variety of threats or risks that a nation could face at any given time without focusing solely on exceptional measures. Therefore, a two-step test can be constructed to examine, firstly, the level of the threat, and secondly, the nature of the threat. This is done to establish if it is an emergency, or a problem that can be solved by standard practices. It is clear that Ullman’s definitions are directly opposed to the traditional military interpretation of security, which is perceived as being an echo from the last century.

[62] Hough (2008) *Understanding global security*,7. Williams (2008) ‘Introduction’,3. Walt (1991) ‘The renaissance of security studies’,212

[63] Hough (2008),7. Terriff. et al. (1999),21. Ullman (1983) ‘Redefining security’,133. Collins (2007) ‘Introduction’,3.

2.2.1 Conceptualising Threats

It is almost impossible to separate threats from security as these two concepts are entwined. However, there is a shift from the construction of threat and security as a state concern to an open-ended approach where the state and non-state actors are involved in security. I have used the following two sections to increase the definitional conceptualisation of central security areas discussed in this thesis. The shift is embedded in cyber-security where the technological weaknesses are exploited by hackers, who directly seek out vulnerabilities in computer systems. Ayoob claims that the threat is linked to vulnerabilities, which threaten or have the potential to bring down or weaken state structure territorial, institutional and governing regimes.[64] Buzan et al. accepts that threats and vulnerabilities are no longer purely linked to military defence, but it has a broader scope.[65] These definitions are important. However, it is necessary to take them one-step further because anticipatory-risk has another scope and this concept has become the operating concept of security and, thereby, it circumvents previous threat-based definitions (chapters 3 to 6).

The way in which cyber-security is conceptualised and managed cannot be comprehended in an analytical framework where exceptionalism is central. Cyber-security fails to be categorised by its normal or exceptional nature. Buzan et al. claims that security issues have to meet strictly defined criteria that differentiate them from the usual run of the merely political.[66] However, I find this definition too narrow. It is a fact, that threats can arise from a number of different sources, and the common determination for threats and security is the way security is framed, perceived and assessed. I also reject the idea that the threat can only be considered within the normal politicised area. Threats can be destructive regardless of their position in the politicised system and the way the discourse is framed. Nevertheless, it is evident that threats are being assessed differently in the global sphere. I support Beck when he correctly abolishes the internal and external dimension of threat. He states that we all are members of a global community of threats and these threats are no longer the internal affairs of particular countries, because one state cannot deal with the threats alone.[67] I claim that a new dynamic develops from the global interconnectivity and dependency on computer technology, because computering is common almost in every-day life and

[64] Ayoob (1995) ‘The third world security predicament’,9. Collins (2010),3. Terriff et al. (1999),18.
[65] Buzan et al. (1998),5. Hough. (2004),8.
[66] Buzan et al. (1998),5. Hough. (2004),8.
[67] Beck (2009) ‘World risk society’,8.

as a result, new threats have surfaced.[68] Therefore, new forms of security measures and governance forms are developed to accommodate the cyber dangers, arising in and from cyber-space, which do not fit the previous threat scenario.

2.2.2 Conceptualising Security

The definition of security is closely linked to threats, and I find it difficult to find a universal characterisation of security despite several attempts to explain and justify the concept. This lack of definition can be transferred to the problem of conceptualising cyber-security in precise terms. Therefore, I outline the common understanding and definitions of security in order to understand the underpinning elements of security. Luciani focuses on an old-fashioned understating of security, where it is defined as the ability to withstand aggression from abroad.[69] Levy supports this argument by linking security to values that need protection.[70] Again, Buzan et al brings in an alternative perspective to the security debate by rejecting the narrow interpretation that security is purely a state concern. Yet, they create a paradox. On one hand, Buzan et al claim that the issue needs to be framed as posing an existential threat to a designated referent object, which does not necessarily needs to be the state, incorporating government, territory or a particular society. On the other hand, Buzan et al still see the state as the primary provider of security as they have the means to ensure the survival of the referent object (section 4.4).[71] From my perspective, cyber-security cannot be pinned down to a pure state problem or related to an external aggression. It is naïve to limit the security framework to the sovereignty of the national state or particular values because cyber dangers cannot be framed in a narrow way because of global interconnectivity. The threats of cyber-attacks are external as well as internal issues, and a clean-cut distinction between these areas cannot be upheld.

Security definitions have become more complex and less tangible; they have become a matter of conditions, rationalities, and interpretations linked to specific security threats.[72] This is a fundamental argument in this thesis, and I argue that the security structure requires a broadly defined security understanding. This is done to encompass the multi-levelled threat structure, which covers a particular way of seeing security

[68] Researchomatic (2013) ‘’Peoples’ dependence on computers technology’.
[69] Collins (2010) ‘Introduction’,3.
[70] Huysmans (1998) ’Security! What do you mean?’,229-230. Levy (1995) ‘Is the environment a national security issue’,40.
[71] Buzan et al (1998),21. Sheehan (2005) ’International security’,53.
[72] Booth (2007) *Theory of world security*,105

problems deriving from everyday practices. Morgan argues correctly that security is a condition, like health or status, which resists easy definition and analysis.[73] This subjective security perception is supported by Valverde, who grasps the complexity of security and the lack of definitions. She argues that security is not something we can have more of or less of because it is not a thing at all. Valverde claims that security is just a name used for a temporally extended state of affairs characterised by the calculability and predictability of the future.[74] This impressive statement encompasses the key element of anticipatory governance central to my security perspective. Job follows on from this argument. The author argues that in principle, four or more securities create problems simultaneously: the security of the individual citizens, the nation, the regime and the state.[75] Job identifies one of the primary concerns regarding cyber-security, where an unbalanced view of security discourses creates problems. The main problem is that different community groups or security actors perceive threats differently, and therefore, knowledge exchange, resource allocations and measures remain insufficient. As a result, uncoordinated security approaches jeopardise the security level because a lack of understanding of the area creates gaps in the security framework. In relation to cyber-security, for example, these conditions allow the security actors to patch the security gaps, but not to solve the underlying issues globally. The main problem is that the governance structure has become a very complex and differentiated perception of the severity of cyber-crime, and its socio-technological impact makes the interplay and competition among the various security actors' problematic (chapters 5 and 6).[76]

Both Wolfers and Booth analyse the subjective and objective nature of security, which is highly relevant in terms of protecting the virtual world. Although the Internet is an imagined free space for the exchange of ideas, we know only a little about online threats and technological developments in the future (section 1.1). As a result, it is only possible to perceive cyber-dangers by using a subjective and objective interpretation, and there are areas that slip through the assessment and categorisation. This follows the argument that complete security does not exist, as this would require that no threat is present.[77] I believe that it is naïve to think that a fully free society, which is built

[73] Terriff et al. (1999),2. Booth (2007),97.
[74] Valverde (2002) 'Governing security, governing through security',85. Zedner (2009),14.
[75] Terriff et al. (1999),20.
[76] Terriff et al. (1999),20.
[77] Zedner (2009),14. Ullman (1983),129. Cf. Rasmussen (2006) *The risk society at war.*

entirely on liberties, can exist without any security measures. Security and liberty are contested concepts, which act as signposts for an ideal, which we seek, but can never achieve. Instead, it is possible to balance the concepts to find a middle ground where security is held in check by the libertarian stance.[78] This discussion is ongoing, and a solution cannot be reached because liberty vs. security can never be objectively interpreted, as the interpretation will always be linked to a certain time and place – and the framing of a particular concern. In this thesis, I promote the understanding that security is a condition that needs to be handled in different ways, either in order to neutralise the threat or to avoid the risks mutating into actual threats. This is in line with Wolfers' security definition, where he focuses on the objective and subjective nature of security.[79] He correctly states that security could be approached objectively where there is a real threat, and subjectively when there is a perceived threat.[80] Booth supports this idea when he argues that security is an instrumental value is at the heart of the political significance of the concept. In order to understand this, three distinctions are necessary: between absolute and relative security, subjective and non-subjective threats, and survival and security.[81]

The definitions above fail to provide a precise and comprehensive understanding of neither threat nor security. Moreover, they do not enhance the understanding of the growing significance of multileveled security, which is useful to comprehend and advance the empirical cyber-security research. Instead, they act as indicators for ways of seeing security as a concept, which give a fragmented explanation of what security can be, and how security can be analysed. To get a conceptual understanding of the parameters used to define cyber-security, I extend the discussion to include in a historical analysis of certain aspects of security. In the following sections, I argue that historical events or paradigms are not only useful for reviewing previous security concerns, but they are also relevant to our understanding of the fragmented and differentiated security perspective, which has transformed over the last century. Interpretations of experience show how the long-term effect of events, security trends,

[78] Cf. Gross (2009) 'Security vs liberty'.
Waddington (2005) 'Slippery slopes and civil libertarian pessimism'. Haubrich (2006) 'Anti-terrorism laws and slippery slopes'. Waddington (2006) 'Terrorism and civil libertarian pessimism'. Zedner (2005) 'Securing liberty in the face of terror'. Gearty (2010) 'Escaping Hobbes: liberty and security for our democratic (not anti-terrorist) age'. Waldron (2003) 'Security and liberty'.

[79] Sheehan (2005),53.Wolfers (1962) ''National security' as an ambiguous symbol',151.

[80] Sheehan (2005),53. Wolfers (1962),151.

[81] Booth (2007),105.

security perceptions, and security changes have influenced the way cyber-security is perceived and governed.

2.3 The Development of Security

Discussions on the issue of threat and security go back in time and have been a topical issue for centuries. Still, it is possible to establish different security models linked to special situations, i.e. war or conflicts. Therefore, it is important to establish how these changes have shaped our understanding of threat and security. By studying the historical evolution, it is possible to create a foundation for discussing cyber-security discourses and management forms relevant for security studies in the 21st century. In Foucault's archaeology of knowledge, the analysis seeks to describe the history of discourse, and how thing are understood with all its interrelations and transformations (section 1.4). Historical analysis is therefore not only related to questions of procedure, but also with theoretical problems.[82] According to Foucault, instead of studying the origin, these archaeologies examine the archive:

> "[S]ystems that establish statements (´enonc´es) as events (with their own conditions and domain of appearance) and as things (with their own possibility and field of use)".[83]

Central to Foucault's way of seeing things in a historical context, is that the systems of thought and knowledge are governed by rules defined by conceptual possibilities developing from ideas and languages used in a given domain and period.[84] Each of these provides meaning to the understanding and the construction of discourses in the current security paradigm. According to Foucault, modernity is not reducible to existence prior to the interpretation of it. Instead, Foucault highlights how 'historical a priors' do not give a priori to all experience, but rather they give attention to experiences that constitute the condition of possibilities of a particular era.[85] These shape the perceptions of particular paradigms; yet, they do not highlight any absolute truth, only a way of seeing.[86]

In line with a Foucaultian analysis of discourses, the concept of security has shifted in response to particular historical events. This development gives particular insight into the understanding of cyber-security, as this security form has shifted in response to

[82] Foucault (1969). Flynn (2005) 'Foucault's mapping of history',30.
[83] Foucault (1969), 128. Flynn, (2005),30.
[84] Foucault (1969). Gutting (1994) 'Michel Foucault'.
[85] Haugaard (2002) 'Foucault',184-185.
[86] Haugaard (2002),185.

particular events. Because of modern technologies, a change in modern warfare from the 19th century created new strategies and ways of understanding security. What happened in and after WWI (1914-1918) had an effect in WWII (1939-1945), and decisions taken in the aftermath of WWII caused the bipolar power struggle during the Cold War.[87] These security conflicts might seem outdated and irrelevant in a cyber-security context, but they are not. Firstly, I argue that it is possible to identify the first trembling and ineffective moves towards institutionalised cooperation as a security management solution, which we have seen accelerate over the decades. In terms of cyber-security, global technological interconnectivity makes it impossible to manage cyber-space without cooperation, different security actors and anticipatory governance forms. Secondly, I argue that there has been a significant development towards individual security deriving from the first attempts to develop rights and freedoms to a personal responsibility to secure cyber-space. Nevertheless, significant changes deriving from the Cold War have broadened and deepened the security agenda, which has created a new analytical foundation for understanding security.[88]

2.3.1 The First World War

First World War (WWI) was described, as the war to end all wars, but this was not the outcome.[89] The war was the result of the industrial revolution during the 19th century, when technological advances had made it possible to develop and use destructive weapons. These new weapons, along with the development of new forms of communication and supply lines facilitated the build up to the first global war.[90] Two important areas of security emerged as a result of the WWI. Firstly, WWI marked a significant shift in international cooperation and the development of the first set of international human rights.[91] In the aftermath of the war, collective security was secured through a new agency, the League of Nations (L.N), which was established in 1919.[92] The main role of the L.N. was to create a forum where states could resolve their disputes instead of aggressively pursuing their own individual interests and ignoring other states.[93] This required that the collective states could oppose aggressive states and use force if necessary, regardless of national interests. It was hoped that the L.N would

[87] Galvin (1991) ‘From immediate defence towards long-term stability’,2. Vedby Rasmussen (2004) ‘It sounds like a riddle’,386.

[88] Roe (2010) ‘Societal security’,203. Buzan and Hansen (2009) *The evaluation of international security studies*,212.

[89] Weiss and Kalbacher (2008) ’The United Nations’,325.

[90] Weiss and Kalbacher (2008),131.

[91] Hirst (2001),81. Smith (2007) ‘Textbook on international human rights’,16.

[92] Gray (2007) *War, peace and International Relations*,268. He (1995) ‘The crucial role of the United Nations in maintaining international peace and security’,77.

[93] Hough (2008),31.

ensure international cooperation, morality, and the diplomatic openness.[94] However, even though all the member countries agreed on this, the essential platform for cooperation was missing, and the lack of an international institutional system with general structures and practices made the L.N. inadequate as a peacekeeping institution.[95] Despite the lack of success, I believe that this marked a step forward in international cooperation and human rights, and it paved the way for establishing the United Nations (the UN) as a cooperative institution in the aftermath of WWII.[96]

2.3.2 The Second World War

The second change in security came about because of the impact of the Second World War (WWII). This war was a direct result of the L.Ns failure to establish an international forum for security and foreign affairs which could deal with global crises such as the economic crisis in Germany and the collapse of Wall Street in 1929. By the end of WWII, it became obvious that changes in modern warfare had created new threats that required a rethinking of security. The mass-deaths and destruction worldwide, along with unconscionable violence and massive human suffering called for further protection.[97] This resulted in the development of collective security to prevent future great-power conflicts, which prompted a rethinking of security to include the protection of national and collective security.[98] I would argue that the two directions, which were the core elements of post–WWII security, were based on a paradox.

The first direction was based on the growing focus on national security and the protection of the sovereignty of the state. In the aftermath of WWII, states and their citizens, hugely mistrusted other states, and security was imposed as a protective measure against international anarchy.[99] This state-centric approach was understandable after the years of terror and horror experienced during WWII, but unfortunately, it was prolonged by the bipolar conflict during the Cold War. The second direction developed as a contradiction to the state-centric approach was an enhanced form of cooperation between countries. For example, the UN was created from the ruins of the L.N.[100] The

[94] Gray (2007),270. Hough (2008),31.
[95] Gray (2007),270. He (1995),77.
[96] He (1995),78.
[97] Weiss and Kalbacher (2010,325.
[98] Weiss and Kalbacher (2008),325.
[99] Lippmann (1943) ‘US foreign policy’,32. Hough (2008),11. Collins (2007),3. Buzan (1991) ‘People, states, and fear’,16.
[100] Anderson (1996) ‘The global politics of power, justice and deathons’,239. Hough (2008),35. Weiss and Kalbacher (2008),327. UN (1945) ‘Charter of the United Nation and Statue of the International Court of Justice’. Anderson (1996),239.

UN (and other cooperative organisations) were created, systematised and institutionalised in order to strengthen collective security and avoid faults made by its predecessor by creating an institutional structure.[101] Furthermore, an international set of human rights was developed under the UN Charter of Human Rights and in the European Region; with the Council of Europe (CoE) developing the European Convention on Human Rights.[102] From a historical perspective, it is understandable why a vast amount of states overcame their scepticism and joined collectives. These states recognised that the benefits of enhanced security cooperation were higher than the cost of independence.

2.3.3 The Cold War

The Cold War (late 1940s–1991) was the outcome of the cold peace established between the winning allies during and after WWII.[103] After WWII, only two superpowers remained; the USA and the USSR. These two superpowers were locked in a conflict of mistrust based on their different capitalist and communist ideologies. Their political differences were non-negotiable and fuelled by a deep mistrust.[104] This kind of war never turned 'warm' and consequently, there was a security setback in promoting and developing global cooperation.[105] A new conflict replaced the fragile peace after WWII, and this kept the security actors in a deadlock, where security was only seen from a military perspective. The use of nuclear weapons against Hiroshima and Nagasaki in August 1945 started the superpowers' weapons escalation which changed the security landscape completely.[106]

During the Cold War, the UN failed to play a significant role. The organisation turned out to be indecisive and grossly incompetent in dealing with conflicts because it was trapped in the same situation as its predecessor.[107] To some extent, this changed after the Cold War when the conflicts decreased. Nevertheless, I believe that despite the bipolar conflict, cooperation moved into the security framework, and different important institutions developed which are important for understanding cyber-governance in the current security paradigm. In Europe, security cooperation developed which resulted in

[101] *These include the Council of Europe (CoE), the European Coal and Steel Community (ECSC), the North Atlantic Treaty Organization (NATO), the Organisation for Economic Co-operation and Development (OECD), and the World Trade Organization (WTO).*

[102] CoE (1950) 'The European Convention on Human Rights'.

[103] Gray (2007),188-192.

[104] Gray (2007), 186.

[105] Towel (2005) 'Cold war',159.

[106] Waltzer (1977) *Just and unjust wars*,263-268, 269-274. Wirtz, (2010) 'Weapons of mass destruction',326.

[107] Hirst (2001) *War and power in the 21st Century*,81.

the creation of the North-Atlantic Treaty Organization (NATO), The Council of Europe (CoE) and The European Union (EU). NATO is a military alliance focusing on external security challenges and providing a framework for military integration. Internal European integration after WWII began with the creation of the European Coal and Steel Union (ECSC) in 1951. The development of ECSC was politically and economically motivated and was based on a treaty system containing both intergovernmental and supranational elements.[108] This community has over the years changed, and today the EU is considered to be an important security player, both externally and internally in the region. The rationale for this cooperation was to restore Europe and prevent Germany from developing once again into a military power.[109] The desire for lasting peace in Europe brought the countries of Europe in a new model of regional and political cooperation.[110]

Despite the fact that this is not a human rights thesis, the concept has relevance by placing human beings central to the security framework (human security), and as a balancing concept to prevent misuse of state power. Human rights were not only developed through international cooperation in the UN. Regionally, the CoE developed a human rights system in 1949, when the European Conventional system launched a set of rights and the court system. [111] After the Lisbon Treaty, the EU launched its system of rights, known as the Charter of Fundamental Rights of the European Union.[112] Although the tendency to involve non-military issues did began to gradually develop from the first set of rights established after WWI, the security perspective was still purely on military security. Nevertheless, the understanding of security was challenged and it slowly began to change through different initiatives. The first significant step towards a new security agenda was launched in the 1970s by the Independent Commission on International Development Issues (the Brandt report):

> “[A]n important task of constructive international policy will have to consist of providing a new, more comprehensive understanding of ‘security’ which would be less restricted to the purely military aspects… Our survival depends not only on military balance, but on global cooperation to ensure a sustainable biological environment based on equitably shared resources”.[113]

[108] Foster (2006) ’Foster on EU law’,8.

[109] Smith (2007),103.

[110] Craig and de Búrca (2008) ‘EU law, text, cases and materials’,3-4. Sheehan (2010) ‘Military security’,176

[111] Foster (2006),7. Cf. Lauren (2011) *The evolution of international human rights*. Smith (2007).

[112] Foster (2010) ‘Blackstone’s EU treaties and legislation 2010-201’,252-259. Cf. Konstadinides and O’Meara (2014) ‘Fundamental rights and judicial protection. Carrera et al (2012) ‘The Court of Justice of the European Union as a fundamental rights tribunal’. Lenaerts. (2012) ‘Exploring the limits of the EU charter of fundamental rights’. Douglas-Scott (2011) ‘The European Union and human rights after the Treaty of Lisbon’.

[113] ICIDI (1980*)* ‘North-South. A programme for survival’,124. Hough (2008),13.

2.4 The Historical Shift in Analysing Security Post-Cold War

The end of the Cold War in the 1990s left the world in a power vacuum, and created a significant shift in analysing security. I argue that the Brandt report prompted a major step towards a rethinking of threat and security, and this fostered a new way of seeing security beyond military defence. As a result, I make a between the post-Cold War's reinvention of security and the fragmentation of security issues, which is central to cyber-security. The Cold War was not followed by another global conflict and therefore, the concept of security expanded to other areas in order to be applicable in times that are more peaceful. Today, non-military problems are causing economic instability, environmental degradation, the dependence on foreign financial resources, mass-migration, organised crime and pandemic disasters.[114] The concept of human security has also developed since the end of the Cold War, and this human-centric security approach emphasises desirable human conditions for people to be secure.[115]

Human security highlights this new direction by integrating individuals in the security spectrum and within the United Nations Development Programme (UNDP), which has promoted this idea.[116] The central idea is to ensure the welfare of ordinary people.[117] Still, it is hard to capture a precise definition and understanding of this.[118] The UNDP has defined human security as:

> "[F]reedom from want and freedom from fear".[119]

Yet, despite this relative vague concept, human security has changed the security perception by focusing on the relationship between individuals and the state – and, in particular, state sovereignty.[120] Newman raises an interesting question of whether it actually is possible to uphold all the right intentions in human security, calling it a normatively attractive but analytically weak concept.[121] Despite the definition problems, the logic behind the individualistic approach has created an alternative to the security framework by breaking the state-centric dominance. Security in the recent paradigm

[114] Cottey (2007),6, 193.
[115] Kerr (2007) 'Human security',123.
[116] UNDP (1994) 'Human development report',22. Wibben (2008) 'Human security',458. Cf. King and Murray (2001) 'Rethinking human security'. Thomas (2000) 'Global governance, development and human security'. Owen (2004) Human security-conflict, critique and consensus'. Thomas and Tow (2002) 'The utility of human security'. Bellamy and McDonald (2002) 'The utility of Human security'.
[117] Paris (2001) 'Human security,87.
[118] Paris (2001),88.
[119] *Freedom from want is a condition where basic needs are met. Freedom from fear is a condition where human dignity is realised*. Poku (2010) 'Globalization, development, and security',258-259.
[120] Newman (2004) 'A normatively attractive but analytically weak concept',358. Ryerson (2010) 'Critical voices and human security,170.
[121] Newman (2004),358–359.

includes both state and individual approach, which is the legacy of this individualistic dimension (chapters 3 to 6).

Security cooperation post-Cold War is characterised as a transitional period; changes are central, and former cooperative structures and institutions are being reinvented to include new threats. The previous construction of threat and security is no longer needed. The UN still struggles to uphold its objectives as a peacekeeping institution and to create the diplomatic foundation for peace. This has created problems, and the consequences were highlighted in relation to the ethnic wars in the former Yugoslavia (1991-2001).[122] During this conflict, the UN showed its inefficiency while peacekeeping on the territory of former Yugoslavia. It was during this intervention that the UN was condemned for participating in the conflict without the political and legal support it required.[123] The result was the same in the conflict in Syria (from 2011), where the UN demonstrated its inability to act to restore peace and security.[124]

Surprisingly, NATO managed to transform itself after the end of the Cold War, when most security experts expected the alliance to disappear, or to simply continue as a bureaucratic organisation to ensure the stability and development into a new security order.[125] No one expected the alliance to reinvent itself and be even stronger than before, but NATO is a leading institution which has constructed a security architecture based on a new reflexive conception (chapter 5).[126] During the same period, a new security agent has developed since the Cold War. After a slow start under the intergovernmental structure, the EU has developed into an internal and external security power.[127] The Lisbon Treaty created a more visible security structure in external affairs, which over time will strengthen the EU's role as a security actor.[128] The cooperation was previously complicated by the intergovernmental structure due to the diversity of the EU Member States' national, foreign and security traditions and priorities. The First Gulf War (1990-1991), the Yugoslavian wars (1991-2001), and the Iraq War (2003) exposed the problem of a lack of common stance in international. The internal

[122].Grey (2007),230. Gray (2004) *International law and the use of force*,218-224. Gray (2007),229-231.
[123] Gray (2007),218-219.
[124] BBC News (2012d) 'Syria conflict: West 'appalled' by Russia China UN veto'.
[125] Fierke (2007) 'Constructivism',178. Vedby Rasmussen (2001) 'Reflexive security',297. Cf. Vedby Rasmussen (2002) ''A parallel globalization of terror': 9-11. Vedby Rasmussen (2004). Vedby Rasmussen (2006).
[126] Vedby Rasmussen (2001),298.
[127] Buzan and Hansen (2009),167.
[128] Cottey (2007),79. Piris. (2010) 'The Lisbon Treaty',170. *Enhanced cooperation between the institutions has been established together with a more visible link between the Common Foreign and Security Policy (CFSP), the European Council (EC), the European Parliament (EP), and the High Representative*. Cottey (2007),60. Foster (2010),12.

disagreements between the Member States were a setback to developing the EU as an important security actor internationally.[129]

2.4.1 The 'War on Terror'

The progress made in the transitional period after the Cold War suffers a remarkable setback in the 'War on Terror' era as exceptional measures was used to circumvent legislation, processes and practices designed to protect individuals.[130] It has been argued that these measures are necessary to manage the actual existential threat by bypassing existing laws and international obligations instead of violating them directly. This is what Ericson calls counter-laws.[131] The use of counter laws follows the logic that:

> "[L]egal order must be broken to save the social order".[132]

By adopting a 'war-like strategy' as the preferred response to terrorism, the U.S. and others have enhanced the political discourse rather than focusing on the rights and obligations covered by different human rights treaties. This way of framing threats and developing governance forms was the consequence of the Madrid and London bombings, where the reaction was an increase in proactive counter-terrorism legislation and practices. As a response to the threat, the Copenhagen School's analytical framework, securitization (chapters 4 to 6), and emergency measures have dominated the security agenda.

This security paradigm has significance for cyber-security and the security governance discussion in this thesis, as this period also bridges the development of cooperation on multiple levels with new and alternative governance forms. It is in this period that the focus on risk begins to mutate, and anticipatory management procedures and practices develop (section 3.7). The starting point for discussing cyber-security and anticipatory governance forms is the acceptance of a changing security structure and the way of seeing and governing dangers. Cooperative networks begin to transform, building on a stronger structure, and acting as incitements for pooling resources and working in partnerships. Following these changes, states recognise that they cannot handle the threat alone, and security formations are being strengthened to counter terrorism and

[129] Cottey (2007),79-80.

[130] Aradau and Van Munster (2009) 'Exceptionalism and the "war on terror",3.

[131] Ericson (2008) 'The state of pre-emption',57. Aradau and van Munster (2009),3. *The first counter-law is known as the law against the law based on the formulation of new laws that undermine existing laws. The second counter-law is called surveillant assemblages where the use of extra-legal technologies of surveillance and profiling undermine established legal norms and standards.* Ericson (2008),57. Hebenton and Seddon (2009) 'From dangerousness to precaution',346. Ericson (2007b) 'Security, surveillance and counter-law',6. Ericson (2007a) 'Rules in policing: Five perspectives',387. Aradau and van Munster (2009),3.

[132] Hebenton and Seddon (2009),346.

other emerging threats. However, the cooperation structure is fragmented, and the security issues are diverse. The events of 9/11 can be understood as a new trademark of transnational terrorism which had been developing since the onset of globalisation. The enemy now was not another state, but rather individual actors who were imbedded in terrorist cells throughout the world. It was now evident that new security strategies were needed to manage these new terrorist threats. Terrorist attacks have previously been associated with a small number of states with unsolved and ongoing political conflicts.[133] However, the 9/11 terrorist attack was a turning point in security and modern warfare. The 9/11 attack was the first-time irregular warfare involving non-state actors was the principal plot line, and this had an immediate effect worldwide. [134]

2.4.2 Risk-Security Paradigm

Following the historical analysis, I argue that three features are noticeable. Firstly, the concept of security has progressed from a state-centric approach to a wider security agenda, which includes states, groups and individuals. This denotes the way in which a variety of security actors is involved in security on vertical and horizontal levels. Secondly, security is not only related to military defence. The development of security has created a diverse agenda, which involves a large number of non-military issues. Thirdly, to manage these threats, cooperation is necessary, because public and private sectors, groups and individuals are equal targets.

With these three elements in mind, I analyse the shift in security by outlining the current security model which has emerged from the Cold War, the 'War on Terror' and globalisation. Complex non-military issues, constraints and social trends were present in previous approaches to security.[135] However, these issues have become more important to the security agenda fuelled by cooperative changes, the focus on individual security, and globalisation.[136] In this thesis, I side with Vedby Rasmussen, who argues that the evolving nature of traditional military security results in security strategies that go beyond the means-ends rationality central to the former security structure.[137] Instead, the core element of security policies contains reflexive management processes based on the perception of the threat imposed and the management of future risks.[138] Heng

[133] Jackson (2005) 'Writing the war on terrorism',93. Cottey (2007),42.
[134] Gray (2007),262.
[135] Heng (2006) 'The 'transformation of war' debate',70.
[136] Heng (2006),70.
[137] Vedby Rasmussen (2006),37.
[138] Hough (2008),55. Vedby Rasmussen (2001),285.

supports this argument by stating that policy-makers consistently use anticipatory measures to avert probabilistic scenarios.[139] This argument is relevant to understand the security patterns in the following discussion.

In modern security strategies, anticipatory governance and practices have been given a prominent place. This management form has mutated from the pre-emptive wars of the last decades - the NATO bombing of Kosovo, the wars in Afghanistan and Iraq - to be deeply integrated in policy-making decisions and security strategies.[140] The former U.S. President George W. Bush (The Bush Doctrine) justified the increased use of anticipatory governance by stating:

> “[I]f we wait for threats to fully materialize, we will have waited too long”.[141]

This is a common justification for including anticipatory governance and practice in security strategies, where the fear of the unknown is the main accelerator. In relation to cyber-security, I believe that there is a notable change in the use of threat and risk strategies, although both are related to uncertainty. As stated by Clausewitz, threat assessment is linked to the enemy’s intentions and their capabilities: [142]

> “The first consideration in the combination of a plan for war is to determine the centres of gravity of the enemy’s power, and, if possible, to reduce them to one”.[143]

I find that contemporary security policies and governance structures are entirely different. They are based on the prospect of managing a future event by setting up preventive barriers to capture risks before they develop and become a greater danger to groups and individuals. Strategies are based on a calculation between probabilities and consequences, and this future-oriented element clashes with past management forms (chapter 3).[144] Nevertheless, these management structures are inadequate to capture risks. Vedby Rasmussen rightly criticises Gray, Mearsheimer and other scholars for their obsession with past strategies.[145] By focusing solely on threats, they overlook the most dangerous threat to security; namely the unexpected.[146] Security practitioners have already recognised this and have created anticipatory management structures that mirror

[139] Heng (2006),69.
[140] Heng (2006),70.
[141] De Goede (2008), 164. Gilmour (2002) ‘Bush: West Point grads answer history's call to duty’.
[142] Heng (2006),71.
[143] Von Clausewitz (1997) *On war*,364.
[144] Heng (2006),71. Vedby Rasmussen (2006),37.
[145] Vedby Rasmussen (2006),28.
[146] Vedby Rasmussen (2006),29.

the risks, i.e. structures that enhance resilience and preparedness. As stated by Clausewitz:

> “Every age has its own kind of war”.[147]

Over the years, an intricate pattern of cooperation has developed, with new alliances being based on significant policy diversity in security areas. This thesis is concerned with the European region. I have chosen this region because it has a history of developing anticipatory measures. These measures span more than two decades as the region has become subjected to large-scale aggressive acts such as terrorism, cyber-attacks, organised crime and the threat of weapons of mass-destruction.[148] The European region has cemented itself as a valuable security player and has developed numerous security institutions and agencies since the end of WWII. Moreover, I have selected Europe because other international institutions have failed to facilitate a global cooperative culture to counter the threats. One reason for the global fragmentation and differentiated approach towards security issues is that security threats are perceived and assessed differently throughout the world. However, Europe has been open to developing alternative governance methods and alliances beyond regional security institutions, such as NATO, the CoE and the EU. This open approach has resulted in new risk-based security formations and structures based on a variety of different, overlapping and complementary forms of cooperation, which go beyond the normal structures. The U.S.-EU, NATO and bilateral or multilateral security agreements are an integral part of transatlantic cooperation, which may or may not include the involvement of the UN.[149] Furthermore, there is a strong tendency to involve private security actors, and this has been emphasised in security strategies developed by the three leading organisations, i.e. Coe, EU and NATO

2.5 Emerging Security Issues in the 21st Century: The Concept of Cyber-security

New types of security threats have emerged during the 21st century, which circumvent the traditional analysis in the threat-security tandem. The current security paradigm calls for a different management structure based on resilience and preparedness linked to risk-management and anticipatory governance and practices. The most recognised new

[147] Vedby Rasmussen (2006),29.

[148] Williams (2008) ‘(In)security studies, reflexive moderniziation and the risk society’,58. EU (2003) ‘European security strategy,3-5.

[149] Cottey (2007),78.

area is cyber-security, which has had an impact on all levels of everyday life, i.e. public and private sectors, and groups and individuals.

Cyber-security is the response to the growing threat of cyber-related crimes, and the concept has developed to provide a safe and secure computing environment for all users. Various international and national institutions have failed to develop a comprehensive definition of cyber-security. This has resulted in a lacuna in understanding cyber-security, where real life activities are combined with the artificial world connected internationally. The International Telecommunication Union (ITU) has tried to create a definition by stating that cyber-security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management methods, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, as well as organisations' and users' assets.[150] Cyber-security attempts to ensure the attainment and maintenance of the security properties of the organisation and users assets against relevant security risks in the cyber environment. It is considered that the general objectives include availability, integrity and confidentiality.[151] I would argue that cyber-security can be seen as an umbrella term for numerous, differentiated and fragmented security risks, all of which share one common factor: the use of cyber-space and the Internet. The definition above shows that the field is too complex for one security actor to deal with. Underpinning the argument in this thesis is that this type of security develops in spaces between different geographical areas, sectors and, i.e. international, regional, national, local, and between public and private sectors.

2.6 Conceptualising Cyber-space Related Crime

In this thesis, cyber-security is the over-arching theme, which often are called cyber-crime (not to be mixed up with the subcategory of cyber-crime). Wall states that the term cyber-crime, or more rightfully cyber-space crimes, will give:

> "[A] greater meaning if we construct it in the terms of the transformation of criminal or harmful behaviour by networked technology, rather than simply the behaviour itself".[152]

Although, I agree with Wall, this is not the accepted terminology in convention, treaties, legislation, journal articles, which all use the confusing term cyber-crime, cybercrime,

[150] ITU (2014).
[151] ITU (2014).
[152] Wall (2007) 'The Internet as a conduit for criminal activity,10.

or cyber-crime randomly. I would argue that the lack of clarity creates unnecessary confusion between the typologies. In relation to this thesis the overall concept is cyber-security rather than the more correct, but confusing, use of cyber-crime for both the overarching form of crime-crime and the sub-unit; cyber-crime. Since the EU cyber-security strategy uses the term cyber-security as the overarching category, I have chosen to follow that in order to avoid confusion. I have made this distinction between the two areas rather than creating an overly defined taxonomy. Over-conceptualising and re-naming can stall the progress and understanding of the concept, which is already widely accepted throughout world, despite their conflicting names.

Yar correctly states that the creation of cyber-space has opened up new forms of criminal acts, where the criminal activity takes place within or by using networks of electronic communication.[153] These criminal networks use the Internet, the dark net TOR and different types of social media, such as Twitter, Facebook, Snapchat and WhatsApp. Eurojust's Annual Report 2011[154] states that:

> "The term "cybercrime" encompasses two types of criminal activity: the use of the Internet to commit "traditional" crimes such as fraud, forgery, publication of sexual abuse material, etc., and the use of electronic means to disrupt or completely immobilise information systems".[155]

Cyber-space is an area where a limited number of activities are visible, and control of the Internet is almost impossible. In the contemporary world, there is a complicated and self-sufficient digital underground economy in which data is the unlawful product.[156] Cyber-space provides different types of criminals with an

> "[I]nteractional space or environment created by linking computers together into a communication network".[157]

Europol has described cyber-crimes in their annual report on Organised Crime and Trend Assessment (2011),[158] as:

> "Internet technology has now emerged as a key facilitator for the vast majority of offline organised crime activity. In addition to the high-tech crimes of cybercrime, payment card fraud, the distribution of child abuse material, and audio visual piracy, extensive use of the Internet now underpins illicit drug synthesis, extraction and distribution, the recruitment and marketing of victims of trafficking in human beings (THB), the facilitation of illegal immigration, the supply of counterfeit commodities, trafficking in endangered species, and many

[153] Yar (2006),155. Cf. Avina (2011),285.
[154] Eurojust (2011) 'Eurojust annual report 2011'.
[155] Eurojust (2011),34.
[156] Europol (2011c),5.
[157] Yar (2006), 155.
[158] Europol (2011a) 'Organised crime and trend assessment'.

> other criminal activities. It is also widely used as a secure communication and money laundering tool by criminal groups".[159]

This report highlights that the wide distribution and availability of technology opens up new ways of committing crimes by misusing cyber-space for personal gain.[160] The speedy developments within this technical environment, and the new ways of communicating have created a new industrial revolution, which has established an information age within late modernity.[161] In addition, I find that the organisation of cyber-space makes this area difficult to manage, as the structure of hacking groups often lack clear leadership. Hacking is delegated according to the hacker's technical expertise, and most members only know each other online (chapters 5 and 6).[162] Online forums are places for the recruitment of up-coming hackers, who operate in the underground economy, and have a degree of organisation which makes it possible for them to work on specific projects.[163]

The most common terms used to distinguish different types of unlawful online activities are; cyber-crime, cyber-warfare and cyber-terrorism. A cyber-related crime could be an organised cyber-attack using malicious software or malware in the form of viruses, worms, Trojan horses or logic bombs.[164] These types of cyber-attacks differ in motivation and activities.[165] However, I consider it impossible to create a clear-cut definition of the three areas of cyber-security, because the illegal actions largely overlap, and the actors can shift between the different groups. Klimburg comes up with an example of the problem of conceptualising the three areas. Klimburg argues that it is mostly impossible to identify whether an attack originates from the North Korean Army, a lonely South Korean student or the Japanese-Korean Mafia. Indeed, all of these entities could have been involved in the same attack.[166] This is because the conceptualising of cyber-crime, cyber-warfare and cyber-terrorism can be a misleading one when they overlap. However, one thing that I do want to highlight is that these concepts do not comply with state-centric structure or governance forms.[167] The important factor is to look at the underlying motives to determine whether an attack is

[159] Europol (2011a),9.
[160] McCusker (2006) 'Transnational organized cyber crime',263.
[161] Yar (2006),3.
[162] Europol (2011c),6.
[163] Europol (2011c),6.
[164] Yar (2006),157-159. Wall (2007a), 225. Clarke and Knake (2010),287. Klimburg (2011) 'Mobilising cyber power',41-42.
[165] Klimburg (2011),41-42.
[166] Klimburg (2009) 'Cyber-attacken als warnung**.**
[167] Klimburg (2009).

carried out for economic or personal gain, is part of an important cyber-warfare campaign/information-warfare or is based on political, religious or ideological reasons.

Cyber-attacks follow technical innovations, with the denial-of-services (DoS) and distributed denial-of-services (DDoS) being the most common. The DoS and DDoS attacks attempt to make a machine or network resource unavailable to its intended users by exhausting their resources, i.e. overloading the mailbox.[168]

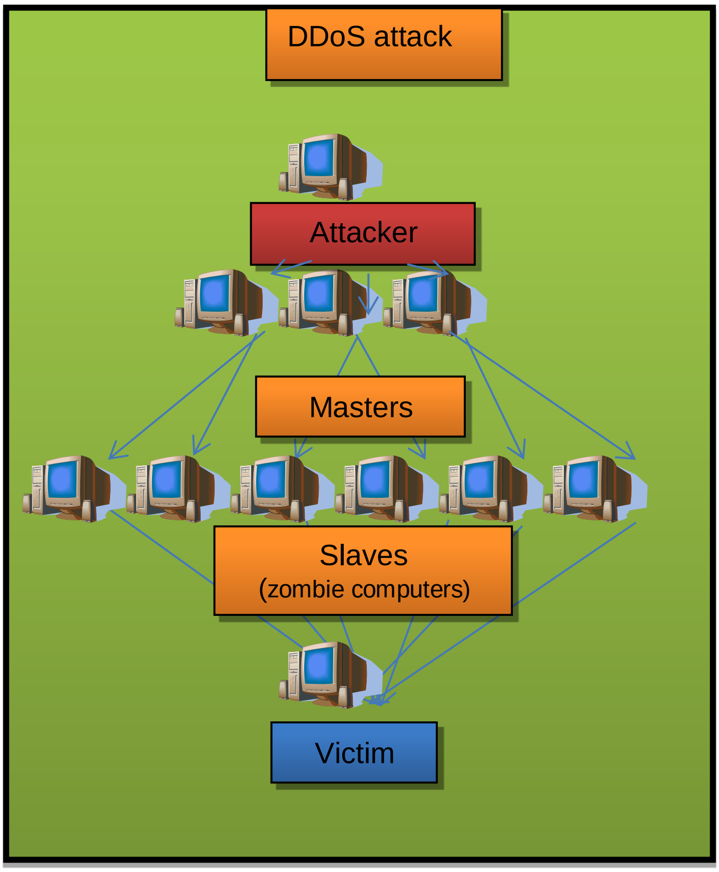


Figure 1 illustration of a DDoS attack

In addition, bugs, worms and viruses are constructed to hit a designated target in order to meet a particular end.[169] The most dangerous type of attack derives from the use of logic bombs.[170] These hidden files or software packages are small and do not need to communicate, making them extremely difficult to locate. Nevertheless, if the bombs are triggered, they can cause a massive amount of destruction.[171] A growing concern is the

[168] Klimburg (2011),42. Yar (2006), 30. Clapperton (2013) ‘Who are the hackers?’. Patrikakis et al (2004) ‘Distributed denial of service attacks’.
[169] Klimburg (2011),43. Yar (2006),30.
[170] Klimburg (2011),42.
[171] Klimburg (2011),42.

extended use of botnets. Botnets draw together a number of computers to empower large-scale attacks by enhancing computer capabilities (chapter 6).[172] The problem with botnets is there are an unknown number computers involved, which makes it difficult to trace the attackers.[173] By using botnets, it is possible to generate a large-scale cyber-terrorism attack that is either carried out with the use of tools affecting significant numbers of information systems (computers), or it is related to attacks that cause considerable damage; disrupted system services, financial cost, loss of personal data, etc. The damage caused by large-scale attacks has a major impact on the functioning of the target itself, and/or affects its working environment.[174] The harm caused by large-scale attacks impacts on the functioning of the target itself, and/ or affects its working environment, which can result in severe economic, political and social costs.[175]

Previously, attacks were carried out in an indiscriminate and non-structured way. These attacks included the non-controlled, worldwide cyber-attacks known as the Love Bug, Code Red and MyDoom, which created chaos throughout the world.[176] Today, attacks appear more controlled, and some have an inbuilt code that can target a certain company, software or area. The Heartbleed bug (2014) is an example of how hackers were able to gain access to sensitive material by spreading a bug through the Internet in a controlled way.[177] The bug is usually considered as cyber-crime, but the same code can be used to obtain information regarding CI, CII and ICTs, to provide information to carry out an attack, which will disrupt or destroy the target. The bug may also have been developed in relation to state-sponsored terrorism or warfare in order to infect the enemy’s computer network, i.e. the Stuxnet attack on Iranian power plants, which set back the program of enriching uranium.[178] South Korea has claimed that they are to develop similar tools in an attempt to damage North Korean nuclear facilities.[179] I would argue that this is a slippery slope, because once the Stuxnet code is recognised as a military weapon, it could be open for trade to rouge states and terrorist groups. The virus and DDoS codes can easily be activated by terrorists, who wish to infect a particular programme used by their intended target. However, attacking by using these

[172] EC (2010a),3. Schmidt (2014) ‘Hierarchies in networks’,189.
[173] EC (2010a),3.
[174] EC (2010a),3.
[175] EC (2010a),3.
[176] Jordan and Taylor (2004),21. Yar (2006),30–31.
[177] *The bug affects web servers running a package called OpenSSL, such as Imgur, OKCupid, Eventbrite, and the FBI's website.* Hern (2014).
[178] NATO (2011b) ‘New threats’. Dunn Cavelty (2013) ‘From cyber-bombs to political fallout’,111.
[179] BBC News (2014e) ‘South Korea to develop Stuxnet-like cyberweapons’.

codes can become dangerous, as there is an enormous risk that these computer weapons can end up causing unintentional damage, way beyond its original scope.[180]

2.6.1 The Typology of Cyber-crime

Cyber-crime is the most common criminal activity, where the virtual world is used to commit unlawful actions. It is necessary to examine the motivation of hackers to distinguish between the three different forms of cyber-related offences. The underpinning rationale for cyber-crime is to:

> "[G]ain access to, and to control over, others' computer systems. Once such access and control have been gained (what hackers call 'taking ownership' of the system), a range of further prohibited activities becomes possible".[181]

Most of the cyber-crimes are similar to those carried out in real life:

Direct or indirect assaults by threats using emails, videos, or phones, this is also known as cyber assaults or cyber stalking, i.e. sending unwanted emails, which are abusive, threatening, or obscene.[182] This may involve electronic sabotage, such as 'spamming' (junk emails) or computer viruses.[183]

Child pornography is the most contentious kind of online pornography. This form of cyber-crime is distributed through the Internet, which provides efficient methods for offenders to send images around the world.[184]

Cyber laundering of illegal funds is a crime, where money is transferred through the Internet in order to turn it into legal funds.[185]

Cyber theft is a very common offense. This is a crime where computers are used to steal through unauthorised access. These activities can be related to cache poisoning, embezzlement and unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism and piracy.[186]

Cyber vandalism is yet another type of criminal activity, where the hack attack directly targets the Internet websites and where the content is altered. The computer technology is used to damage or destroy data. [187]

2.6.2 The Typology of Cyber-warfare

Cyber-warfare/information-warfare takes different forms, which go beyond the use of cyber-crime as a criminal enterprise.[188] Rid has claimed that there will never be a global cyber-war.[189] However, I strongly disagree with Rid's argument. I would argue that just

[180] BBC News (2014e).

[181] Yar (2006),27.

[182] Uda (2009) 'Cyber-crime, Cyber-terrorism, and Cyber-warfare in Perspectives',3.

[183] Ellison (2001) 'Cyber Stalking',141.

[184] Uda (2009),3. Wall (2007), 109,112.

[185] Uda (2009),3.

[186] Uda (2009),3.

[187] Yar (2006),29. Uda (2009),3.

[188] John and David Ronfeldt (1993),145. Cf. Dipert (2010) 'The ethics of cyber-warfare'. Carr (2012) *Inside Cyber Warfare*. Knapp and Boulton (2006) 'Cyber-warfare threatens corporations'

[189] Rid (2012) 'Cyber war will not take place'

because we have not yet seen any large-scale global cyber-attacks, this does not mean that they will not happen in the future. In the 21st century, it has become clear that cyber-warfare adds a new dimension to military security and warfare strategies.[190] Military warfare is becoming computerised and military means and methods are becoming technologically advanced. For example, the use of drones is now integrated within military strategies. Another example is Israel's aerial shield with its Arrows III interceptor missile designed to deploy kamikaze satellites known as kill vehicles. These missiles are designed to track and crash into ballistic missiles above the earth's atmosphere.[191] This system was allegedly inspired by former US President Ronald Reagan's Star Wars program, the Strategic Defence Initiative (SDI), which was firstly initiated in 1983.[192]

Direct cyber-attacks are part of an ongoing war between states. Yet, unlike traditional warfare, cyber-attacks are not dependent on the best-trained solders or an army that has the most weapons. Instead, successful cyber-attacks are dependent on those who utilise the best hackers and have the most developed technological capacity. Another area of cyber-warfare is introducing malware or hacking sensitive areas of CI, CII and ICTs to obtain confidential information through espionage. Indeed, e-espionage has an indirect impact in the long term as groups or states can use the information to attack vulnerabilities in computer systems. The motivation is different as the sole purpose is to obtain information secretly, but it can also overlap with cyber-terrorism where espionage may be used to obtain information about a particular target (chapter 6).

Beyond the direct involvement of computer technologies in weapons, the use of cyber-warfare covers specific types of illicit actions:

> **The threat of proprietary or confidential information**. Hackers may gain unauthorised access in order to steal or copy information.[193] This is different from cyber-crime as the motivation is not economic or personal gain, but to obtain information to be used in cyber-warfare.
>
> **System sabotage, alteration and destruction**. This can be done as a prank, protest or to display skills, which is part of an ongoing conflict.[194]
>
> **Espionage.** The software is launched to determine the system's weaknesses and to target it. Damage producing software is yet another tool in the information war.[195]

[190] Feng (2015) 'Among Snowden leaks, details of Chinese cyberespionage'.

[191] Williams (2014) 'Israel tests Arrow missile shield, sees Hezbollah threat'.

[192] MacAskill (2010) 'US 'Star Wars' lasers bring down ballistic missile'. Hartung (1998) 'Reagan Redux'.

[193] Yar (2006),28.

[194] Denning (1999) *Information warfare and security*,29.

2.6.3 The Typology of Cyber-terrorism

Cyber-terrorism is the use of different computer networks to harm/shut down CI and CII, to spread propaganda, or to communicate.[196] The growing dependency on information technology gives the terrorists a chance to approach targets, which otherwise would be out of their reach. The more dependent the public-private sectors have become on technology, the more vulnerable it will be to future cyber-attacks.[197] If CI, CII or ICTs are attacked, it could lead to a total breakdown on multi-levels of society if no contingency plans are developed beforehand.[198] Cyber-terrorism is not defined by unlawful activities for personal or economic gain as cyber-crime, nor is it about obtaining secret information linked to cyber-warfare. However, cyber-crime and cyber-warfare can be side-effects or be a part of the terrorist activities depending on the motivation for the attack.[199] Cyber-terrorism is a traditional form of activism, turned into hacktivism using computer-technologies. However, this area is not clearly defined because there is no identifiable actor that characterises cyber-terrorists, nor is it possible to pinpoint their activities, as there are no limits for the use of ICTs.[200] The people involved in hacktivism can be rough states, terrorists, disgruntled insiders, private companies and political activists.[201] Yet, cyber-terrorism is not only a state concern. Although there have been a significant increase in the number of cyber incidents between 2010 and 2015 which have targeted governmental computer systems, a number of these attacks have shown that private infrastructures can also be a target for terrorists (appendix 5).

The most typical of these offenses are:

> **Attacking targets that deliver CI/CII.** This is especially directed towards loss of power due to attacks on systems, which control and manage power grids. This can be power, water, the air traffic, electronic commerce, emergency services and national defence. This can also involve disruption of computer access to certain areas concerning the attacked area, i.e. the Anonymous group's attack on Amazon, Visa, PayPal and MasterCard.[202]

[195] Dipert (2010),391.
[196] Weimann (2005) *Cyber-terrorism*,129.
[197] Weimann (2005),130.
[198] Yar (2006),53.
[199] Denning (2000) 'Cyberterrorism, testimony before the special oversight panel of terrorism committee on armed services',2.
[200] *Jordan and Taylor (2004),39.*
[201] *The UN's declaration on measures to eliminate international terrorism annex to UN (1994) General Assembly Resolution 49/60, and the EU (2002) Framework Decision on combating terrorism.* EU (2002) 'Framework decision on combatting terrorism'.
[202] Laville (2012) 'Anonymous cyber-attacks cost PayPal £3.5m'. BBC News (2010d) 'Pro-Wikileaks activists abandon Amazon cyber attack'.

> **Disruption of financial transactions.** This is another ‘weapon’, because it can bring the economic system to a halt, as commercial transactions, banking and finance can have a substantial impact on the welfare on every level of the state, i.e. Estonia 2007.
>
> **Theft of secret information** regarding defence and national security can also be significant, as to access essential information in those areas can make it possible to carry out physical attacks in reality. This is an important pathway for hackers in order to manipulate and control these entities.[203]
>
> **Crippling the transport system**. Corrupting or crashing control computers or networks.[204]

I have included an analysis of cyber-terrorism in the second case study, which is a sub-category of cyber-security. In contemporary security strategies, it is recognised that the interconnectedness of global CI, CII and ICTs calls for an extensive networked formation to enhance resilience and preparedness including providers and states, whose infrastructure can be targets or used to route attacks.[205] The lack of information regarding cyber-terrorism makes it an interesting area for my analysis in chapter 6. It has been characterised as a new form of war, which we only understand in vague terms. Daily life revolves around the digital world, using the Internet, computers and mobile phones. As a result, it is expected that the providers of devices, Wi-Fi and broadband take steps to maximise the protection against attacks, and there is a similar expectation towards governments and security institutions that they will do the same. Experts are warning against the blindfolded belief that these actors can provide an entirely comprehensive protection.[206] Although there has not been a significant cyber-terrorism event so far, it has become an increasing problem in relation to spreading propaganda and hiring jihadists for IS in Syria and Iraq. This terrorist organisation openly uses the Internet to raise awareness and distribute its ideology to young people through web pages and social media.[207] Moreover, IS uses social media to distribute images of their atrocities, such as the beheadings of hostages.[208]

[203] Yar (2006),53. Grabosky and Stohl *(*2010) *Crime and terrorism,* 38. Goodman et al (2007) *Cyberspace as a medium for terrorists*,195.
[204] Yar (2006),53.
[205] Tikk (2011) ‘Ten rules for cyber security,123.
[206] Dorgan (2013) ‘Cyber terror is the new language of war’.
[207] Siddique (2014) ‘Jihadi recruitment video for Islamist terror group Isis features three Britons’.
[208] Ackerman (2014) ‘Islamic State militants claim to have killed US journalist James Foley’. Lewis et al (2014) ‘Steven Sotloff: Isis video claims to show beheading of US journalist’. McCurry (2015b) ‘Isis video purports to show beheading of Japanese hostage Kenji Goto’. Chulov (2015) ‘Jordanians turn their minds to revenge after Isis killing of pilot’.

Cyber-terrorism is not only linked to attacks in and through cyber-space. The Internet is the primary facilitator for spreading propaganda and communication, and it can be a powerful tool for mobilisation and radicalisation.[209] It is noteworthy that the terrorist organisation IS has adopted these computer technologies and communication forms, and used them as a corporation for marketing their cause.[210] However, the actions of terrorist organisations are impossible to measure, and no one knows the scale of the use of the Internet as a communication tool between terrorists and/or other organised crime groups.[211] Another area of cyber-terrorism is introducing malware or hacking sensitive areas of CI, CII and ICTs in order to obtain confidential information through espionage. Espionage has a similar indirect significance in the long term as the groups can use the information to attack vulnerabilities in computer systems. The motivation here is different, as the sole purpose is to obtain information secretly, which overlaps with cyber-warfare (chapter 6). However, the groups do not necessarily act in secret. It can be a part of their brand to tell the world about their activities online. Groups, such as Anonymous and LulzSec, often hack just for fun, or draw attention to particular issues by disrupting websites or launching DDoS. Group Anonymous also has an accomplished record of leaking e-mails and other material obtained from some of its targets.[212]

2.7 Conclusion

In this chapter, I outlined the relevant security approaches and definitions, and given a historical outline of the understanding of security from WWI up to the current security climate as a part of a Foucaultian analysis. This chapter creates an underpinning foundation for understanding the development of threat-security/risk-security and cyber-security based on anticipatory governance forms. The chapter provides the background, context and definitions necessary for addressing the research objective and the first sub-objective (section 1.2). In the first part of this chapter, I have made a summary of the historical context and background to outline the concept of security and its definitions. The discussion covers a definitional exposition of some of the key concepts. As outlined, cooperation has developed rapidly over the last century. Nevertheless, it is possible to establish the distinctive changes in a historical context, and I have

[209] Siddique (2014). Tran and Weaver (2014) ‘Isis announces Islamic caliphate in area straddling Iraq and Syria’. Tran (2014) ‘Who are Isis?’.

[210] Tran and Weaver (2014). Snow (2014) ‘Isis beheading videos: the scariest part is how well their propaganda is working’.

[211] Europol (2011b) ‘TE-SAT 2012’,11-12. Miller (2014b) ‘Can Iraqi militants be kept off social media sites?’

[212] The Economist (2014b) ‘Hackers Inc. Cyber-attackers have multiplied and become far more professional’

investigated how international society has slowly formed international security agencies. Different historical conflicts have led to changes in states and non-state actors’ involvement in security and cooperation. I believe that knowledge regarding the different shifts in security is useful for understanding the different parameters included in the emerging cyber-security framework. In the current risk-security paradigm, everything can be perceived as a risk, and this enhances the need for a reflexive security structure (chapter 3). The whole security construction has become very complicated and blurred as different alliances, and cooperation are established, and this is very visible in cyber-security, which covers all possible dangers related to cyber-space. In this context, I have chosen to conceptualise cyber-security and the sub-categories to enhance the understanding of the anticipatory responses and governance forms, which are incorporated in this emerging security area.

3 Perspectives on Security Governance. Nodal Governance, the Concept of Risk, and the use of Anticipatory Governance

3.1 Introduction

Cyber-security problems call for new critical approaches to understanding technological and societal risks emerging from this area, and future policy challenges can only be addressed when we identify the nature of the problem appropriately. In this chapter I reviewed the literature from the perspective of its usefulness in both answering the research question and in its ability to generate insight into the governance structure of a particular security area. Cyber-security is an area that has so far been under-researched. As a result, it is important to focus on the concepts relevant for discussing cooperation, security actors and anticipatory governance. I have chosen to use three perspectives, nodal governance, the concept of risk and anticipatory governance to discuss cyber-security governance. The underpinning foundation of this thesis is that the cyber-security management structure is embedded in nodal governance, and this creates, albeit in a hybrid form, the institutional framework for managing multileveled cyber-security. This chapter enables me to progress the security discussion to the following parts of this thesis by outlining how cyber-security is governed, the underlying concepts and defining anticipatory governance. In addition, I have investigated the way in which anticipatory governance is designed to employ foresight in the creation and execution of plans and actions in the policy process.

Through this lens, it is possible to analyse cyber-security governance. I have also discussed the concept of risk, which has developed to be the preferred security response to managing cyber-space. Under this umbrella term, anticipatory governance and practices are tools used for increasing security of fundamental technological and societal uncertainties. I have developed the discussion by bridging the gap between present and future knowledge in order to enhance resilience and preparedness towards cyber-risks. The chapter is organised as follows: Firstly, I discuss governmentality and nodal governance, as these are fundamental to understanding and executing cyber-security management and implementation of governance forms in the European region. Secondly, I review the academic literature to define the significance of the concept of risk in order to understand the way in which anticipatory governance is organised. Thirdly, I explore the concept of anticipatory risk and proaction to illustrate the position of imagining future scenarios and execute changes ahead of possible cyber-attacks. In this section, I investigate security structures developed to manage risk on different levels in an ongoing cycle.

3.2 The Theoretical Foundation for Cyber-security Governance

Securing cyber-space has become one of the major challenges at the beginning of the 21st century. The increasing use of risk in cyber-security covers a growing norm, where interconnected computer technologies are seen as fundamental to economics, government, society and culture.[213] Yet, security actors perceive the risks from different perspectives, which subject cyber-management to constant reviews in order to manage the future.[214] Cyber-security covers many different security aspects, spanning from a state-centric approach to individuals as first-line security actors. Therefore, a flexible understanding of security management is vital to embrace all these different aspects. The use of governance in this thesis refers to the move from the traditional command-and-control approach towards governance form, where people and institutions become central beyond the detailed and compartmentalised regulation from the top.[215] Tait et al states that integrated or joined policy approaches are needed to remove contradictions, inconsistencies and inefficiencies caused by policies or regulations.[216] To address these issues, I have chosen to use nodal governance as the foundation because this governance structure is deeply rooted in cyber-security. This concept is based on the work of Shearing, Burris, Johnson, Wood, Dupont, and it acts as a signpost for understanding the mixture of governance forms and practices developed by numerous actors.

Nodal governance is based on the mentalities, governance forms, and the associated technologies of different nodes brought together in a hybrid network.[217] Complexity and diversity are an integral part of governance, and they are commonly used to describe nodal networks. Anticipatory governance and practices are created within the nodes, which are established to manage unlawful online activities ad hoc. The participants are selected because of their specific knowledge regarding the security issues and management forms. In cyber-security, the standard security processes are diverse, consisting of the Internet, public-private partnerships, markets, informal policy

[213] Deibert and Rohozinski (2010b),29. Garland (2003),59.

[214] Ericson and Doyle (2004),141.

[215] Lyall and Tait (2005b) ‘Shifting policy debates and the implications for governance’,3. Cf. Barben et al (2007). Bevir and Rhodes (2003) *Interpreting British governance*. Newman (2001) *Modernising governance.* Tait et al (2004) ‘Governance, policy and industry strategies’.

[216] Cf. Tait et al (2004). Tait and Bruce (2004) ‘Global change and transboundary risks’.

[217] Foucault (2009),115-134. Cf. Lemke (2000),2. Lemke (2001) ‘The birth of bio-politics’. Gordon (1991) ‘Governmental rationality’. Burchell (1991),90.

networks at the international level, and the whole spectrum of public and private governmental initiatives.[218] The essential point when moving the security studies agenda forward is to focus on the relationship between shifting concepts and changing practices – what Foucault calls regimes of power/knowledge.[219]

The focus on the 'unknown unknowns' has taken precedence in security where imaginative worst-case scenarios are increasing in order to enhance resilience before events spins out of control.[220] A large number of risk and security scholars, such as Aradau, Holling, O'Malley, Reid, Rose, Rogers and Coaffee, and Walklate and Mythen, have critically analysed the concept of resilience under the risk-management umbrella, and it is clear that this concept is incorporated in the anticipatory governance process of responding to the challenge of the 'unknown unknowns'.[221] The critical understanding of these academics and the research of resilience and preparedness covers a variety of areas within security studies and risk, which are important in order to understand the proactive element incorporated into cyber-security and anticipatory governance and practices. The difficulties, of managing cyber-space and the Internet, derive from the assumption that the virtual world is anarchic (chapters 1, 2). Therefore, cyber-space is not only seen as ungoverned, but it is also structurally ungovernable because it does not have the familiar boundaries of physical space that usually surround security and state structures (section 1.1).[222]

Figure 2 illustrates the way in which this thesis is drafted in order to answer the research objectives. The discussion progresses through the lens of nodal, where I focus on the European governance structure and the cyber-security apparatus. In the next chapter, I introduce two security schools into the cyber discussion. The two schools have different ways of seeing security, which enhance the understanding of cyber-security, highlight the limitations in existing security policies, define critical areas and gaps and generate useful knowledge from their critique.

[218] Burris et al (2008).

[219] Cf. C.A.S.E. Collective (2006).

[220] Dasse and Kessler (2007) 'Known and unknowns in the 'War on Terror'.

[221] Aradau (2010), Aradau and van Munster (2008). Aradau and van Munster (2007), Burgess (2007) 'Social values and material threat'. Coward (2012) 'Between us in the city'. Lakoff and Collier (2010) 'Infrastructure and event'. Lundborg and Vaughan-Williams (2011) 'Resilience, critical infrastructure, and molecular security'. Brassett and Vaughan-Williams (2015). O'Malley (2012). Lentzos and Rose (2009). Walklate et al (2013). Walklate et al (2013b) . Coaffee et al (2008) 'The everyday resilience of the city'. O'Malley (2010) 'Resilient subjects'. Petersen (2011). Reid (2012) 'The disastrous and politically debased subject on resilience'. Lentzos and Rose (2009). Evans and Reid (2013) 'Dangerously exposed'.

[222] Barnard-Wills and Ashenden (2012) 'Securing virtual space',117.

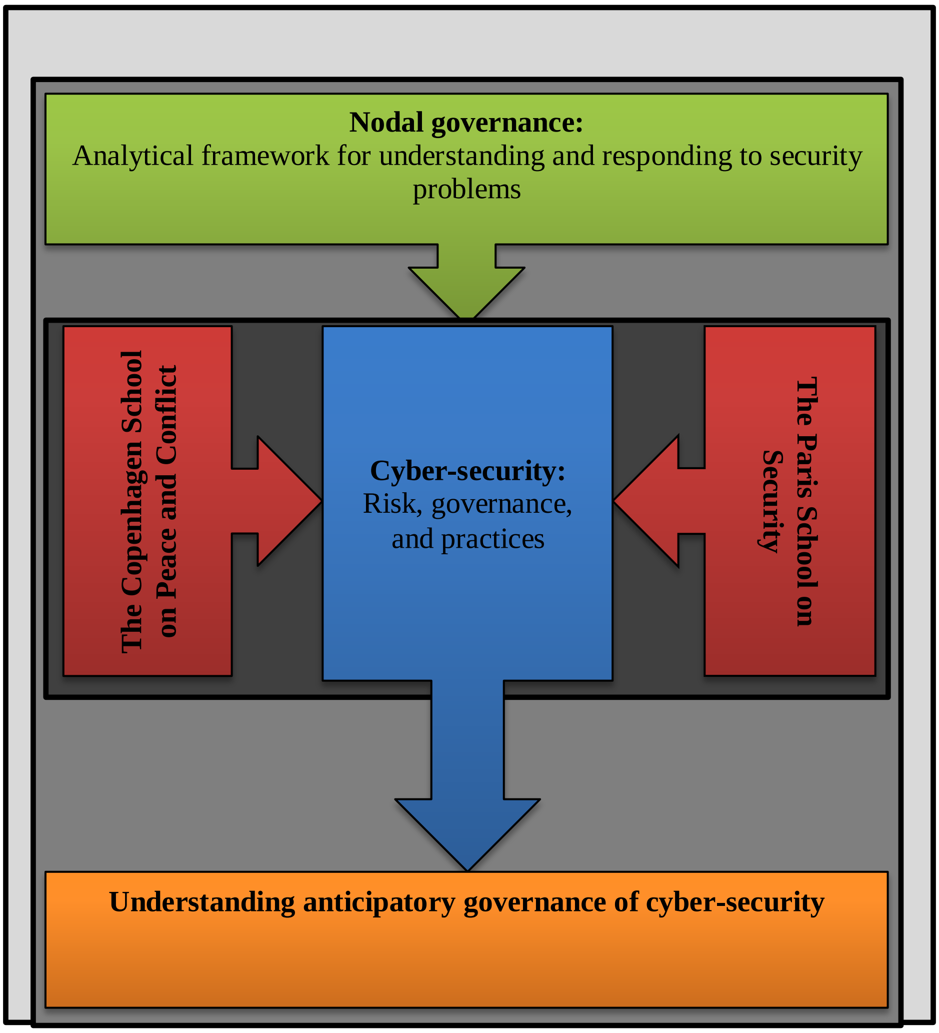

Nodal governance:
Analytical framework for understanding and responding to security problems
The Copenhagen School on Peace and Conflict
Cyber-security:
Risk, governance, and practices
The Paris School on Security
Understanding anticipatory governance of cyber-security

Figure 2 model for advancing the discussion

These two differing perspectives are necessary to examine contemporary cyber-security strategies and their governance forms in the European region. I have chosen the European region, firstly, because three of the world's most significant security institutions cover this geographical area, i.e. NATO, the CoE and the EU (appendix 1). Secondly, the three European security institutions are at the forefront of developing anticipatory responses to the growing cyber-threat. However, internally in the region, the EU are the most proactive cyber-security actor, and the institution has developed legislation, action plans, guidelines, and practices to enhance cyber-security. Additionally, it has a strong institutionalised framework, which is missing in other regions, institutions, and ad hoc formed cooperation. Based on a literature review, I argue that cyber-security in the European region can be conceptualised as produced by various networks of actors in a transnational and national, and public and private context. In part two, I investigate how these security actors manage to address the shifting cyber-security concepts and practices in an area where the technological development challenges the perception of security.

3.3 Governmentality and Nodal Governance

To discuss cyber-security, governance and security actors, I need to clarify the way in which I approach security and cooperation developed from a Foucaultian interpretation of governmentality. In this thesis, the way I think of security, and how is it governed derives from this analytical framework. This analytical framework explains the different parameters involved in governing practices, from state regulation to self-defence/self-regulation. Governmentality is based on contemporary practices of governance combining 'govern' and 'mentality'. The term government refers to a more or less systematised, regulated and reflected mode of power exercised over others, which follows a more specific form of reasoning. Therefore, government covers:

> "[T]he regulation of conduct by the more or less rational application of the appropriate technical means".[223]

Foucault introduces a differentiation between power and domination. He insists that:

> "[W]e must distinguish the relationships of power as strategic games between liberties – strategic games that result in the fact that some people try to determine the conduct of others – and the states of domination, which are what we ordinarily call power. And, between the two, between the games of power and the states of domination, you have governmental technologies".[224]

In cyber-security, numerous forms of governance and practices have been developed to cover a legislative lacuna (sections 5.4, 6.4). This includes a variety of networks, such as state and non-state actors, who develop different techniques of governance. Moreover, there is a high level of self-governance included in the framework, as all computer users have a responsibility to ensure a certain level of security. I believe that governmentality is useful to analyse and understand fragmented and differentiated cyber-security governance forms and practices. It is important to look at the way in which these actors frame cyber-threats and respond to the growing number of threats. It is also important to investigate the different management possibilities which create alternatives to standard policy areas, because of the technological and social dependency on computer technologies in everyday life. As a result, the management

[223] Hindess (1996) *Discourses of power*,106. Lemke (2000),5.

[224] Foucault (1988). 'The ethic of care for the self as a practice of freedom',19. Lemke (2000),5.

structure includes an increasing number of actors, who all have different incitements and knowledge about protecting critical infrastructure (CI), critical information infrastructure (CII), and information computer technologies (ICTs).

According to Foucault, government is defined as the conduct of conducts of individuals, collective bodies, and organisations created in a flexible and autonomous way.[225] This has been explained as:

> "Conduct is the activity of conducting (conduire), of conduction (la conduction) if you like, but it is equally the way in which one conducts oneself (se conduit), lets oneself be conducted (se laisse conduire), is conducted (est conduit), and finally, in which one behaves (se comporter) as an effect of a form of conduct (une conduite) as the action of conducting or of conduction (conduction)".[226]

The citation above contains a double meaning: the activity of conducting an individual and his/her relations, and the way individuals are being conducted or conducting themselves. The 'conduct of conduct' is essential when looking at security and behaviour likely to be regulated by rules, practices and processes.[227] Dean correctly argues that governments are to some extent a calculated and rational activity, which is undertaken by a multiplicity of authorities and agencies. These authorities and agencies employ a variety of techniques and forms of knowledge used to sharpen the conduct by working through the actors' desire, aspiration, interest and belief (chapters 4 to 6).[228]

Institutions seek, through a range of actors, to obtain order and discipline using a set of values and customs in combination, which constitutes different areas of social capital.[229] The central issue in governmentality is the circulation of discourses, where all activities involve a particular level of powers and governance.[230] Foucault describes the use of practices as:

> "[W]ith the aim of grasping the conditions that make these acceptable at a given moment: the hypothesis being that these types of practices are not just governed by institutions prescribed by ideologies, guided by pragmatic circumstances – whatever roles these elements may actually play – but, up to a point, possess their own specific regularities, logic, strategy self-evidence, and "reason". It is a question of analysing a "regime of practices" – practices being understood here

[225] Dale (2004) 'Governance, governmentality and the OMG',181.
[226] Foucault (2009),19, 193.
[227] Foucault (2009),19.
[228] Dean (2010) *Governmentality*,18. Rose et al. (2006),86. Cf. Garland (1997),175.
[229] Mythen and Walklate (2006) 'Criminology and terrorism',385.
[230] Mythen and Walklate (2008) 'Terrorism, risk and international security',229. Mythen and Walklate (2006) 'Beyond the risk society',384-385.

> as places where it is said and what is done, rules imposed and reason given, the planned and the taken-for-granted meet and interconnect".[231]

According to Rose, O'Malley, and Valverde, governmentality is:

> "[O]ne that seeks to identify these different styles of thought, their conditions of formation, the principles and knowledge that they borrow from and generate, the practices that they consist of, how they are carried out, their contestations and alliances with other parts of governing".[232]

The analytical perspective of governmentality is separated from the theory of power, authority and governance. Using governmentality analysis allows me to ask particular questions about the issues which I seek to understand through the empirical investigation.[233] Rose and Miller propose a nominalist approach to the governmentality analysis, and this creates a contrast to the realism model based on a direct objective link between input and outcome (sections 1.4, 4.9).[234] Rose and Miller claim that the analysis is used to isolate programs, rationalities and technologies, and to examine the forms of discourses, knowledge and subjectivity, which are entailed in these.[235] I include this viewpoint in my own analysis of cyber-security, where an objective analysis leaves out the level of uncertainty central to cyber-security and anticipatory governance. Cyber-security includes too many unknowns, which makes it impossible to analyse from a pure objective perspective, as we need to imagine the missing pieces to make the unknown known. Instead, to anticipate the future, this area is framed subjectively and objectively by viewing the threat and the different responses isolated in relation to managing each possible risk.

3.3.1 Nodal Governance

In the previous chapter, an historical outline based on Foucault's archaeology of knowledge has shown how security has developed from being a pure state concern to a pluralistic security approach. This outline supports the claim that there has been a fundamental shift in the security arrangement. Today, security involves transnational and cross-sectoral organisations, groups and individuals beyond the use of referent objects (chapters 4 to 6). Nodal governance takes its beginning in the fragmented and differentiated security construction, which has emerged in the last couple of decades by

[231] Foucault (1994) 'Questions of methods', 225.
[232] Rose et al (2006),84.
[233] Rose et al (2006),85.
[234] Healy and Perry, (2000),119-120. Cf. Guba and Lincoln (1994). Tsoukas (1989) 'The validity of idiographic research explanations'.
[235] Rose and Miller (1992) 'Political power beyond the state',177. Garland (1997),183.

moving security from hierarchical governance structures to heterogeneous strategies.[236] Nodal governance is based on the exercise of power and the involvement of various agents. There is an extended focus on these agents, and because of the way security is perceived, governments are forced to involve state and non-state actors in security management. This means that the study of governance is concerned with the means of calculations, the governing authority or agencies, and the different types of knowledge and techniques involved.[237] Rose and Lentzos state that this is a part of the Foucaultian way of thinking about governmentality, where new technologies are invented or deployed in an ongoing circle to improve security.[238]

Wood and Shearing highlight that security actors are structured, as there is not one single model of governance. Instead, nodal governance is formed by complicated hybrid arrangements and practices, which merge governmentality with various institutional arrangements. This governance form relates to a complex set of relationships in which ‘steerers’ and ‘rowers’ creates collaboration and align their interests.[239] Fundamental for contemporary security governance is the understanding that when the modern state rules, it does not rule alone. Instead, it works in the background of an elaborate network of relations. These different nodes are situated in a complex of institutions, organisations and apparatuses, which involves states and non-state actors, i.e. regulatory state bodies, international institutions and agencies, self-regulating bodies of industry and private companies (chapters 5 and 6).[240] These security actors are seeking to govern the activities of numerous quasi-autonomous initiatives within the security apparatus.[241]

Shearing et al point out that nodal governance is based on a special way of thinking about matters, such as governing nodes, methods for executing the influence over the events, resources to support the management, management of a given problem, and institutional structures.[242] According to Wood and Shearing, governing auspices covers two sides: They are both objects of governance, and actors who govern directly or through others.[243] Fundamental to these governance forms is the development of

[236] Foucault (2009),115-134. Lemke (2000),7.
[237] Dean (2010),18.
[238] Lentzos and Rose (2009),233-234.
[239] Wood and Shearing (2007),21. Burris et al (2008),3. Cf. Burris et al (2005) ‘Nodal Governance’. Crawford (2006) ‘Networked governance and the post-regulatory state?’. Bayley and Shearing (2001) *The new structure of policing*. Osborne and Gaebler (1992) *Reinventing government*.
[240] Miller and Rose (2008),55. Amoore and de Goede (2005),150. Lentzos and Rose (2009),233
[241] Lentzos and Rose (2009),233-234.
[242] Wood and Dupont (2006) ‘Introduction’,3.
[243] Wood and Shearing (2007),27.

different associations between multiple actors from traditional cooperative agencies and institutions from outside of the established security arrangement. It is not enough to analyse governance structures through political rationalities in which the discursive field and the exercise of power are conceptualised.[244] Miller and Rose correctly highlight that governance should also be analysed in terms of their governmental technologies. This is based on mundane programs, calculations, techniques, apparatuses, documents and procedures developed in the nodes to manage complex areas, such as security.[245] I position knowledge, capability and resource exchange central to activities within the nodes, where governance is a domain of cognition, calculation, experimentation, and evaluations based on projects, plans and methods.

Burris et al suggest that the use of both public and private governance has a substantial collective effect. I recognise that it is problematic having both sectors incorporated in the framework. This argument is based on the fact that there is a significant democratic deficit between the stake security actors have in decisions, i.e. their capacity to influence, or be protected (chapters 4 to 6). This claim is fundamental to the understanding of security because this causes problems on the international and local level because there is often an unequal relationship between the resources available, knowledge, and the ability to deal with the externalities of problems to which the actors have little or no control.[246] After reviewing the literature on cyber-security, I recognise that the nodal construction involves actors beyond the state; citizens take part in the new governmental and hybrid institutions, just as they are involved in improving the security level through self-governance of own actions (chapters 5 and 6). These actors are also significant players in overseeing security, i.e. community policing, set local budgets and monitor public expenditures. Although these non-governmental organisations are not as wealthy or efficient as private corporations, they are still important players in different ways. However, I need to mention that governance is not only reserved for responses to security. Criminal networks, like Al-Qaeda, IS, Group Anonymous, or other organised crime syndicates are seen as agencies of governance.[247]

[244] Miller and Rose (2008) ‘Governing the present’,55.

[245] Miller and Rose (2008),55. Lentzos and Rose (2009),233-234.

[246]Burris et al (2008),4.

[247] Burris et al (2008),4.

3.3.2 Indirect Governance

Governing through multiple security actors is linked to Foucault's governmentality. The idea of multiple objectives that need to be aligned is based on Foucault's argument that governance is the right distribution of things for a convenient end. This is only possible if a plurality of suitable actors can be brought into sufficient arrangement to allow the objectives of governance to be realised.[248] This is what Rose and Miller calls the profusion of shifting alliances.[249] I regard changing cooperative entities to be paramount to cyber-security because different risk requires different alliances and regulatory forms. Managing cyber-space and digital technologies cannot be forced into one single form, nor can one actor or agency be responsible for developing anticipatory governance and practices. However, through changing arrangements it is possible to design nodes that have the right knowledge to manage one risk ad hoc. Therefore, nodal governance takes prominence in the cyber-security management combining direct and indirect governance, although this does depend on the way that actors frame and respond to the security issue. Indirect governance is related to market mechanisms - or contractual governance as Crawford has argued.[250] This is also relevant when discussing public-private partnerships, which forms an important part of the cross-sectoral analysis of this thesis. Previously, the command-and-control approach had been the principal regulatory tool, where the state had a defined role in setting goals, monitoring fulfilment and realigning disagreements.[251] However, the governance arrangement has changed to a networked governance structure with multi-agency cooperation working across traditional boundaries.

At present, the state has a tendency to outsource parts of security to other actors, such as private companies and organisations.[252] In the current security paradigm, it is impossible not to involve a range of different security actors, as the risks are ever-present not just directed towards the state (section 4.8). Cyber-security follows this trend, where everyone with access to cyber-space and computer technologies can be at risk. This is interlinked with the management structure, as it is important to include private security actors with specific knowledge of security risks and pre-emptive

[248] Foucault (1991) 'Governmentality',93. Wood and Shearing (2007),19.
[249] Rose and Miller (1992),174. Wood and Shearing (2007),19
[250] Crawford (2003) 'Contractual governance' of deviant behaviour',844. Loader and Walker (2006) 'Necessary virtues', 166.
[251] Crawford (2006),452.
[252] Wood and Shearing (2007),20.

technologies, which are valuable to security governance. As correctly argued by Miller and Rose:

> "Political power is exercised today through a profusion of shifting alliances between diverse authorities in projects to govern a multitude of facets of economic activity, social life, and individual conduct".[253]

Marketisation is not limited to the delivery of security outcomes on a local/national scale, but has become a part of a worldwide market, where security services are undertaken routinely through contractual arrangements.[254] Loader claims that the contractual and market processes have had the effect of commodifying governance, which is bought and sold in the marketplace.[255] However, it does not stop there. In terms of cyber-security, there is a profound desire from private corporations and businesses to protect their computer technologies and critical infrastructure by developing anticipatory governance to increase resilience and prepare for an attack. This makes corporations or organisations relevant security actors who operate outside of contractual relations to public security actors. The inclusion of different sectors has resulted in an extended hybrid structure, which is neither public nor private; where public authorities have embraced private management structures and governance forms, and where private industry has taken responsibility to enhance security.[256]

Wood and Shearing argue correctly that the security application has changed. For them, the state is no longer the sole power actor in the security framework, but rather an equal member of the nodal governance.[257] Loader and Walker, who have a very critical attitude towards the concept of nodal governance, have contested this stance.[258] Their argument is normative rather than analytical, claiming that there is a distinction between the factual involvement of multiple security actors, and to what extent these actors should be involved in. Loader and Walker claim that the extended use of nodal governance makes the state look like an 'idiot'. Consequently, the state appears unable to exercise its power, and the bureaucratic construction is unable to make 'good' on its well-intentional promises.[259] I disagree with this argument. From my perspective the

[253] Miller and Rose (2008),53.

[254] Wood and Shearing (2007),18. Cf. Singer (2003) *Corporate warriors*. Avant (2005). *The market for force.*

[255] Loader (1999) 'Consumer culture and the commodification of policing and security',373-392. Wood and Shearing (2007),18

[256] Dupont (2006) 'Power struggles in the field of security',87. Cf. Johnson, (1992) '*The rebirth of private policing.* Dupont et al (2003) 'The governance of security in weak and failing states'. Crawford and Lister (2004) *The extended policing family'*,21.

[257] Johnson (2006) 'Transnational security governance',34. Crawford (2006), 458. Amoore and de Goede (2005),150.

[258] Johnson (2006),48.

[259] Loader and Walker (2006),172.

nodal discussion is not about the state being unable to exercise its power, but is about who has the skills, knowledge and technical toolkit to manage the threats. From my perspective, the state can still have a central position in some areas, and outsource other areas to private actors by using knowledge, capacity and resources from other agents, such as other institutions, groupings or individuals.[260] Security is also developed purely outside the scope of the state, where groups and individuals develop security strategies to manage other security threats.

Leander also contests the use of private security actors in the nodal structure because of their overarching economic interest in being involved in security. Leander argues that the aim of the state is to protect its population, territory and vital interests in order to uphold its sovereignty, whereas the involvement of private actors in security is driven by other incentives. Economic gain is the main incentive for private actors, but this does not signify that these different actors cannot work towards a common goal (sections 5.6, 6.6). Private actors have already been cooperative parties for years in the market-based neoliberal governance model.[261] Loader and Walker argue that the involvement of other security has opened the door and allowed those actors with 'the loudest voice' and 'the biggest pockets' to organise security. This is done in a manner that extends the insecurity of others in an unjustifiable way.[262] I would suggest that this is a fair point to raise in relation to cyber-security. The whole NSA and GCHQ scandal has revealed that there are problems internally with security agencies, which compromise the privacy of states, groups, businesses and individuals.[263] Leander stresses that it is important to remember that private actors, such as private military companies, are not mere armaments of a governments' policy. They are also individuals and corporations, who follow a market related agenda.[264] The competition in the private market forces the private security actors to lobby their cause with policy-makers, and thereby influencing the policy-makers' view of security.[265]

Johnson contradicts these arguments, stating that there can be situations where the governments' lack of knowledge hinders effective governance in some areas or levels.

[260] Wood and Shearing (2007),14.

[261] *The neoliberal doctrine of minimizing the state where the state should give priority to controlling inflation, deregulate the private sector, and reduce public spending and taxation*. Kjær (2004) 'Governance',130.

[262] Loader and Walker (2006),166.

[263] Ball et al (2013) 'Revealed: how US and UK spy agencies defeat internet privacy and security' Gellman and Soltani (2013) 'NSA tracking cellphone locations worldwide, Snowden documents show'

[264] Leander (2005) 'The power to construct international security',807.

[265] Leander (2005),815.

Johnson highlights the fact that the state outlines the general regulatory principles for the security governance. Under these circumstances, the government does not need to have a particular preference for a particular community.[266] I believe that the arguments, which are for or against nodal security, are relevant, and it is up to the security actors to strike a balance between their different interests. In the risk-security paradigm, both state and non-state security actors have an important role to play, as the distinctions between sectors, to some extent, are eliminated. This is a significant element in cyber-security, where individual computer users are first-line security actors, and everyone has the responsibility to protect CI, CII and ICTs. To do so, it is necessary to push differences aside, and agree on security strategies for the areas where the participating parties have a mutual security interests (chapters 5 and 6).

Nevertheless, the nodal framework is very complex and differentiated and I believe the biggest challenge is to create a system, which includes important check and balancing systems. Accountability is considered one of the essential principles, which is increasingly used in political discourses, in order to convey the idea of transparency and trustworthiness.[267] Accountability is about accounting for past action as well as preventing similar incidents from happening in the future. In first instance, accountability is related to regulation and the way in which the risks are seen and responses are framed.[268] Scholars, such as Scott, Mulgan, Lodge, Marshaw, May, and Smith have discussed the blurring boundaries between regulation and accountability, which some have tried to separate.[269] However, I support Scott's argument that these are linked concepts, which are operating in a continuum.[270] This does not indicate that they follow the same model or structure or is the steering tool in the same way as regulation.[271] From my perspective, the complexity of nodal governmentality and the blurred boundaries between external-internal and public-private creates a serious problem. In this context, power is transferred between nodes, international organisations - and from public to private actors in an obscure mixture. The state-centric model has

[266] Johnson (2006),49.
[267] Bovens (2007) 'Analysing and assessing accountability: A conceptual framework',448.
[268] Seddon (2010) 'Rethinking prison inspection',264.
[269] Scott (2000) 'Accountability in the regulatory state'. Mulgan (2000) 'Accountability: An ever-expanding concept?',555-573. Smith (2009) 'Citizens oversight of independent police services',264. Cf. Lodge (2004) 'Accountability and transparency in regulation'. Jordana and Levi-Faur (2004) Politics of regulation'. Marshaw (2006) 'Accountability and institutional design'. May (2007) 'Regulatory regimes and accountability'
[270] Scott (2000).
[271] Seddon (2010),264. Cf. Bovens (2007).

vanished; instead, a problematic structure arises, which is so complex that it loses the oversight dimension in the process.

3.4 Risk, Anticipatory Governance and the Concept of Resilience

Anticipatory governance and the use of resilience and preparedness in International Relations and security studies are relatively new. Despite this, the subject area has emerged within a wide range of academic disciplines over the years.[272] However, there is increasing concern within the field of security studies about the link between resilience and security with the related concept of risk and anticipatory governance.[273] In the aftermath of the terrorist attacks 9/11, it is possible to see a pattern in the increasing activities about emergency advice, disaster planning, and preparedness. Since the attack, security actors have actively been engaged in imagining worst-case scenarios, developing plans and governance forms which can address uncertain futuristic and technological realities. Dunn Cavelty et al have correctly argued that across various policy fields, resilience has emerged as a universal mode of thinking about the relationship between unpredictable subjects and their complex environment. This links cyber-security and the concept of risk together because the basic assumption about the insecurities of a subject is not only dependant on its vulnerabilities, but also dependent on the subject itself and its ability to uphold stability, survival, and safety of the individual, society, nature, and technical systems.[274] Cyber-security policies are all based on resilience, prevention and preparedness, which position risk centrally within the framework by descending threat-based policies to a secondary place.[275] As a result, threat policies and measures are only relevant as the last resort when anticipatory governance proves inadequate to capture the risks (figure 6).

In this thesis, I have focused on the use of resilience and preparedness as responsive techniques to enhance security of infrastructure, i.e. CI, CII and ICTs (sections 1.3, 3.7 and 3.8). The high level of uncertainty in cyber-security and the focus on possible future events links together security, the concept of risk and resilience and preparedness in order to capture cyber-risks in the constantly changing technological environment. Formulated as a response to the problem of surprising events, the concept of resilience and preparedness draws attention to the changes of epistemic regimes of

[272] Walker and Cooper (2011) ‘Genealogies of resilience’. Holling (1973) ’Resilience and stability of ecological systems’.
[273] Brassett and Vaughan-William (2015),33. Cf. Amoore and de Goede (2005). Aradau and Lobo-Gurrero, Van Munster (2008) ‘Security, technologies of risks, and the political’, Petersen (2011).
[274] Dunn Cavelty et al (2015),4.
[275] O’Malley (2012),8, 10. Lentzos and Rose (2009),243. O’Malley (2010),489.

ignorance/secrecy and risk/uncertainty in a complex world where the new and unexpected are always present.[276] The key to addressing longstanding problems in security practices in emerging computer technologies is the ability to foresee, identify and act upon different cyber-risks before they develop into actual threats. The concept of resilience promises answers to these problems, and at it provides a basis for engaging uncertainty and introducing anticipatory governance forms to manage the risks.[277]

I have given the concept of resilience and preparedness a significant place because of its close link to the concept of risk and the growing use of anticipatory governance in policymaking (sections 3.7 and 3.8). Although it is a rather broad concept, there is academic literature within the fields, such as human geography, sociology and security studies, which are useful to understand and analyse existing cyber-security governance and practices. In this context, critical security scholars, such as Aradau, Lentzos and Rose, O'Malley, Reid and Evans, Rogers and Coaffee, and Walklate and Mythen have a developed a substantial body of work that covers vulnerabilities in systems, communities, individuals, infrastructure, and institutions (section 3.8.1).[278] In order to answer my research objectives, I have narrowed down my primary research area to cover anticipatory governance and practices developed to enhance the protection of CI, CII and ICTs (appendix 6). Security actors constantly assess vulnerabilities and develop responses by imagining worst-case scenarios, whereby possible scenarios are hypothetically played out in order to minimise cyber-risks.[279] I believe that it is impossible to make a clear-cut distinction between risk, resilience and security and the protection of systems, groups and individuals, and infrastructure because the modern lifestyle is based on access to CI, CII and ICTs (chapters 5 and 6). As a result, resilience is fast becoming a mantra of anticipatory governance and security policymaking across a wide range of security risks. The increasing focus on risks in security necessitates contingency planning to protect, maintain and ensure that online activities can continue despite an attack.[280]

Infrastructure covers a complex mix of networks, technologies, systems, sites, facilities and businesses that all deliver goods and services to people, and thereby, support the

[276] Aradau (2014) 'The promise of security',87.
[277] Dunn Cavelty et al (2015),5.
[278] Aradau (2010) . Coaffee et al (2008). O'Malley (2010). Petersen (2011). Reid (2012). Lentzos and Rose (2009). Evans and Reid (2013).
[279] Mythen (2015), 51
[280] Brassett and Vaughan-Williams (2015),32-33.

state, the economy and social well-being (appendix 6).[281] Imagine, for example, a scenario where the infrastructure or computer technologies suddenly break down. There would be no electricity, no heating, no water, no money flow, no tele communication, no online services available and no access to personal data. The realities of such an attack are nearly impossible to predict. For example, the Estonian cyber-attack (2007) was a wake-up call, and European security institutions, governments and private companies realised that there were huge consequences to developing an advanced information society.[282] In Estonia, hackers blocked websites and froze the entire Internet infrastructure i.e. banks, official documents and email accounts.[283] The attack was a revelation internationally because it became evident that it was possible for hackers to shut down a country's infrastructure. Today, this cyber-attack is seen as a 'taster-session' and it outlines how vulnerable society is if infrastructures, such as CI, CII and ICTs, are attacked. This attack increased the pressure on policymakers, security actors and individuals to develop governance forms and practices in order to manage future cyber-risks. In practice, this means that a number of security actors, groups and individuals aim to decrease technological vulnerabilities by introducing a number of anticipatory rules, regulations and practices to manage risks and to recover after an attack. As a result, security actors and providers of CI, CII and ICTs have increased resilience building towards possible cyber-dangers long before they have occurred in an attempt to influence them long after they have happened.[284] I find that this growing use of resilience and preparedness planning under the concept of risk interesting as it constitutes a never-ending circle of security-management and rethinking of security-strategies and measures (section 3.8.1).

In the following sections of the literature review, I will elaborate further on the different concepts and their interconnected relationship concerning the concept of risk, anticipatory governance and the use of resilience and preparedness in cyber-security.

3.5 Conceptualising Risk

Nodal governance has set out an overarching foundation, and the concept of risk provides the actors with a way of seeing and responding to the dangers in and from

[281] Brassett and Vaughan-William (2015),39.

[282] Tikk (2011), 119. EC (2008) 'Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems',2. EC (2010c) 'Commission to boost Europe's defences against cyber-attacks'. BBC News (2007) 'Estonia hit by 'Moscow cyber war'.

[283] BBC News (2007) 'Estonia hit by 'Moscow cyber war'.

[284] Durodie (2004) 'The limitations of risk management',19. Walklate et al (2013) 'States of resilience and the resilient state',186.

cyber-space before they spin out of control. In this thesis, I focus on risk in opposition to previous threat-based security strategies. The movement away from threat-based policies is the result of a long process, where risk has become the policy-makers′ preferred strategic model to anticipate future events (section 2.4.2).[285] Metaphorically, I compare risk-security with a domino effect. If no preventive barriers are in place to stop the risk from mutating to other areas, the result will be catastrophic on multiple levels. This development is a result of the activities of hackers, which requires transnational responses (section 1.1). However, it does not stop here; cyber-risks include a cross-sectorial element because cyber-attacks are directed for a multitude of reasons, i.e. personal and economic gain, espionage, disruption and destruction (section 2.6). Therefore, new problems become non-linear in their causation, and their anticipated consequences become irregular in time and space.[286] The global networked structure of security empowers both groups and individuals in society; it breaks down traditional hierarchies and creates new power structures. The information revolution has been fuelled by new techniques and the process of globalisation, which have both acted has a catalyst for changes in the traditional hierarchy and power structure.[287]

Beck has a very dark and negative vision of the future. He claims, that:

> "[W]e is living on a volcano of civilization".

This citation highlights that Beck sees the risk society as a catastrophic society due to industrialisation.[288] In this context, modernity itself has created threats to society because the side-effects ('bads') are the result of industrialisation's focus on profit and the side-effects of techno-economic development.[289] These 'bads' are likely to transform and strike back like a boomerang, causing damage in an unpredictable way.[290] I follow Beck's argument that the management of cyber-space is based on an obsession about risk-preventing as the world becomes more focused on the negative risks and the prevention of 'bads'. Yet, it is hard to predict these 'bads' in a constantly transforming cyber-world, where individuals are increasingly dependent on computer systems and networks. The technology development has such character that it is only possible to imagine a limited number of worst-case scenarios based on the particular knowledge in present time. Today, we are more afraid than ever because the focus on risk has

[285] Cf. Clauset et al (2007) 'On the frequency of severe terrorist events'.
[286] Beck (2009),177.
[287] Dunn Cavelty and Mauer (2009),128.
[288] Garland (2003),74.
[289] Beck (1992),12-13. Aradau and van Munster (2007),92.
[290] Beck (1992),37. Ericson and Doyle (2004),136.

increased, as the use of technology and technological uncertainties have surpassed our ability to control development.[291] Technological developments bring about new types of future risks that require constant rethinking of security measures and procedures.

Although Giddens understandably rejects the end of the world rhetoric of Beck, he argues that risks is a product of the society's preoccupation with the future (and with security) – and this generates the growing awareness of risk.[292] The social world is organised in a conscious way, which creates greater uncertainties than ever before.[293] I agree with this standpoint. As cyber-space and computer technology has changed, reality is increasingly being overtaken by the artificial world.[294] Ericson and Doyle state that attackers intentionally induce the uncertainty of randomness, which applies to not only victims, but also those who fear becoming a victim.[295] The idea of a growing obsession with risk avoidance is promoted by Furedi, who argues that anticipate future risks have become an important issue in the political debate and social action. Thus, it has become thoroughly politicised issue.[296] Garland follows the same line of argument arguing that these new hazards and dangers are the result of new processes and technologies. Garland believes that skills used to create the dangers will also be able to create technologies and control systems, which would be able to manage the new risks effectively.[297] Yet, if these technologies are to some extent inadequate, there will be a call for more conservative precautionary approaches.[298]

3.6 Defining Risk

Risk has previously been defined as:

> "[T]he probability of an event multiplied by the magnitude of losses or gains associated with the event".[299]

To conceptualised risk, I use the overarching definition of the concept, which is:

> "[T]he product of the probability and consequences (magnitude and severity) of an adverse event [i.e. a hazard]".[300]

[291] Gardner (2009) 'Risk. The science and politics of fear',8. Aradau and van Munster (2007),92.
[292] Lupton (1999), 73. Giddens (1998) ''Risk society',27. Mythen (2004),140.
[293] Giddens (1995) 'Living in a post-traditional society',59.
[294] Giddens (1995),59.
[295] Ericson and Doyle (2004),145.
[296] Furendi (2005) 'Culture of fear',2.
[297] Garland (2003),76.
[298] Garland (2003),76.
[299] Lupton (1999) *Risk,* 8, Douglas (1990) 'Risk as a forensic resource',2. Beck (1994),29.
[300] Lupton (1999), 8, 17-18. Cf. Douglas (1990), 2. Zinn (2008b) 'Glossary',221 O'Malley (2009),5. Burnett and Whyte (2005) 'Embedded Expertise and the New Terrorism',1. Aradau and van Munster (2008),23. Beck (1994),29. Furendi (2005),2. Garland (2003),76. Lopes (1987) 'Between hope and fear: the psychology of risk',255. Borodzicz

The term risk refers to a functional relationship between probabilities and consequences, whereas, uncertainty is linked to the possibility of occurrence.[301] Dean claims that the risk is a way of ordering reality by rendering it into a calculable form.[302] Slovic and Weber develop Dean's argument by saying that risk is seen as a concept invented by human beings to help them to understand and cope with dangers and uncertainties of life. [303] The concept of risk can be used or misused depending on its relations and the rationale for the different combinations. As a result, O'Malley argues that it is important to look at different areas separately. He correctly claims that we should envision risk techniques in terms of variable configurations, assemblages or ensembles of factors, rather than as fixed types.[304] Luhmann perceives risk to be the existence of closed systems, where human societies are structured in a variety of self-organising systems that define their reality and their way of seeing risks.[305] I agree with these arguments, because risk takes different forms and shapes, and it is changeable depending on its relations. However, I find it necessary to analyse risk-management structures to enable me to position anticipatory governance in nodal governance.

3.7 Risk-Management

Risk includes a cognitive map for colonising the future, and the adoption of 'not-yet' events by simulating precautionary actions against imagined harm.[306] As a result, risk has become a force for global political and individual mobilisation, where the future is anticipated from speculative risk scenarios to avoid the unwanted consequences that may emerge.[307] Beck has rightly argued that risk has become a worldwide problem, where states face an equal uniform set of non-quantifiable, uncontrolled risks in all the different areas involved.[308] This does not mean that the various types of risk can be assessed equally. The formation of risks derives from their different historical backgrounds and their different cultural and political systems.[309] The spread of geographical risks are hard to measure and manage, as security problems in one place

(2005),16. BusinessDictonary (2015) 'Risk. Definition'. Haimes (2006) 'On the definition of vulnerabilities in measuring risks to infrastructures',293.

[301] Renn (2008) 'Risk governance',12.

[302] Dean (1999),131. Dean (2010) *Embedded expertise and the new terrorism*,206.

[303] Slovic and Weber (2002) 'Perception of risk posted by extreme events',4. Sjöberg et al. (2004) 'Explaining risk perception',10. Zinn (2008a) 'A comparison of sociological theorizing on risk and uncertainty',174.

[304] O'Malley (2004) 'Risk, uncertainty and governments',24. Steele (2004) 'Risk and legal theory',83.

[305] Renn (2008),31.

[306] Heng (2006),74.

[307] Heng (2006),74.

[308] Beck (2002),42.

[309] Beck (2002),42.

tend to affect other areas (domino effect). In a globalised world, risky events can occur anywhere and put security management under pressure.[310]

Insecurities are the driving force behind the extended use of risk and anticipatory measures in the security strategies. It is clear that most security issues are being managed under the risk umbrella rather than focusing on threats. Uncertainty has a prominent place, and it referrers to situations where risk cannot be organised, and where reliance is linked to subjective methods of estimating the future.[311] This process signifies that the estimations of exposure to risk are non-probabilistic.[312] However, techniques such as risk categorisation and risk assessment are useful elements in transforming unknown threats, hazards or dangers into known threats. Additionally, future construction will itself contain an element of uncertainty because the management of risk is based on past information interpreted today.[313] The central problem is to determine the level of uncertainty. Will this particular event happen or will it remain a risk? By definition, the harm is not certain to materialise; yet, it does not mean that the risk is not real. Nevertheless, different management techniques can help establish some form of data, even though it only covers parts of the puzzle.

3.7.1 Risk Perception

Risk is considered to have a transformative nature, growing in the uncertain space and only made visible through a process of perception and categorisation. I argue that this is a slippery concept because the risk perception continually changes.[314] In this context, risk refers to a multidimensional concept where the perception varies among social and cultural groups.[315] Risk derives from a particular understanding of individuals, groups or communities, which can be risk-adverse, risk-neutral or risk-seeking depending on the problem.[316] Thus, it is impossible to find a common denominator for risk, which is based on individual perceptions.[317] What is a risk, and how do we determine that something is a risk? We need to put meaning into this multifaceted concept to make it possible govern this concept. Risk covers a broad scope, and the use of risk depends on

[310] Ericson and Doyle (2004),145.
[311] Zinn (2008b),221.
[312] O'Malley (2009),5. Cf. Burnett and Whyte (2005),1. Aradau and van Munster (2008),23.
[313] Beck (1994),29.
[314] Hacking (2003) 'Risk and dirt',33.
[315] Renn (2008),21.
[316] Garland (2003),55.
[317] Renn (2008),21.

our own knowledge and interpretation. Garland has given a description of risk in a rather poetic way, stating:

> “Risk is calculation. Risk is a commodity. Risk is capital. Risk is technique of government. Risk is objective and scientifically knowable. Risk is subjective and socially constructed. Risk is a problem, a threat, a source of insecurity. Risk is a pleasure, a thrill, a source of profit and freedom. Risk is the means whereby we colonize and control the future. ‘Risk society’ is our late modern world spinning out of control”.[318]

The citation from Garland illustrates the claim that risks can be all or nothing, and it is determined from case to case and time to time.[319] I suggest that alternative governance structures are required to manage, develop and understand the different risk-based parameters. This creates intellectual and political challenges in rethinking security based on political, economic and societal changes. Included in the process are the technological progress and the skills of the hackers, which put pressure on the existing system (section 1.1). However, I recognise that the main problem is that risks are perceived differently through the world, which then creates an unbalanced relationship (chapters 5 and 6).

3.7.2 Risk Assessment and Risk Categorisation

Closely linked to risk perception is risk assessment and categorisation, and because of the high level of uncertainty, it is important to calculate the likelihood of risk occurrence. Douglas states that the risk turns uncertainties into probabilities.[320] Therefore, the concept of risk is a blurred and complex notion. The difficulty of preventing risks and the problem of defining risks derive from risk itself, its perception, its transboundary nature and the lack of precise predictions about the future. These different elements constantly mutate and transform. Garland explains the high level of uncertainty as:

> “Risk begins where certain knowledge ends”.[321]

Rumsfeld’s famous speech from 2003 regarding the ‘unknown unknowns’ emphasises the problems of uncertainty and unpredictability:

> “The message is that there are no “knowns”. There is a thing we know that we know. There are known unknowns. That is to say, there are things that

[318] Garland (2003),49.
[319] Hacking (2003),40.
[320] Douglas (1986) ‘Risk acceptability according to social science’,19. O’Malley (2004),18.
[321] Garland (2003),52.

> we now know we don't know. But there are also unknown unknowns. There are things we don't know we don't know".[322]

This statement enhances the understanding of the dynamics of risk, and it highlights the fact that risk can be divided into two categories. Firstly, there are risks that are known and manageable. Secondly, there are risks that need to be known as they emerge as unintended consequences of something. From my security perspective, this problem creates a vision of risk as a Chinese box; where there are several unknown areas encapsulated within which are already known, but are just waiting to be opened. These risks can only be known using existing knowledge to construct the reality of the risk waiting to be assessed.[323] However, to clarify the high level of uncertainty, Rumsfeld continued his speech by explaining the 'unknown unknowns' is a metaphor, saying that the absence of evidence is not the same as the evidence of absence. This statement signifies that just because the evidence is missing, it does not mean that the issue does not exist. However, when the assessment is complete, we only have the first two pieces of the puzzle, rather than all three.[324]

3.7.3 Governing Risks

Risk-management is a way in which we govern and how we are governed by particular constructions.[325] Risk derives from knowledge and, therefore, the framing of risks can be dramatized, minimised, transformed or denied depending on who makes the analysis and for what purpose.[326] Beck argues that risk gains meaning from other factors as risk is based on the assumption of relations of definitions. He rightly says that the relations of definitions are principles in different areas, which can decide on data, knowledge, proof, culprits and compensation.[327] Garland further develops Beck's relations of definitions argument, stating that the risk is conditional because the construction is based on underlying conditions. Therefore, risk is understood in relation to what is considered a threat. There will always be a risk of something, for someone, which is estimated for a particular exposure.[328] Consequently, risk cannot be freed from a subjective analysis, and this supports my argument that the risk is subjective, conditional and changeable. Rose rightly claims that the risk is a multiform and

[322] Rumsfeld (2002) 'Press conference by the US Secretary of Defence'. Burnett and Whyte (2005),1. Aradau and van Munster (2008),23.
[323] Beck (1992),34.
[324] Rumsfeld (2002).
[325] Amoore and de Goede (2008),9.
[326] Lupton (1999),29.
[327] Beck (1995) 'Ecological politics in an age of risk',182. Mythen (2004),68. Beck (2009),33.
[328] Garland (2003),53.

heterogeneous combination of rationalities and technologies, which enable us to govern the future.[329] Following on from Rose, I argue that risk is a construction made by human beings within a particular context. The interpretation of risk is significant in relation to cyber-security, where the focus is on future events; something 'we' have no scientific knowledge about, but still attempt to render and calculate.

There is an ongoing debate about whether the risk can be controlled or managed. Lupton has described the western concept of risk as a matter of control.[330] Ewald follows Lupton's argument about risk being linked to control, by arguing:

> "To calculate a risk is to master time, to discipline the future".[331]

Beck contradicts this by stating that past social arrangements are inadequate to control risks. Control is no longer possible in a risk society; instead, it is an act where the risk

> "[B]alancing its ways along beyond the limits of insurability".[332]

I do not consider the risk as being something that is possible to control due to the level of uncertainty. There might be minor and isolated areas that can be monitored. However, the overarching significant features of risks are its shifting ability, where the perception of risk constantly changes along with the related conditions.

Beck claims that the hidden but central issue in the world risk society is how to feign control over the uncontrollable risks in all aspects of life, i.e. in politics, law, science, technology, economy and everyday life.[333] In this context, Beck argues that it is important to understand that uncontrollable risk as not being linked to a particular area, a particular agent, or controlled on the level of the national state.[334] Inspired by this, Vedby Rasmussen correctly states that the risk society has lost control over risks, as they constitute a never-ending process. However, this creates a definitional struggle over the scale, level and urgency of the risk.[335] Adams has rightly criticised the traditional understanding that modern concepts of risks aim to develop management plans to eliminate risks. Adams points out that it does not remove the risks by imposing plans, developing governance structures or by improving the training of human operators. It might be possible to prevent one individual accident, but the level of risks

[329] Aradau and Van Munster (2007),97. Rose (2001) 'The politics of life itself',7.
[330] Lupton (1999),3. Cf. Lund Petersen (2011) 'Risk analysis',703.
[331] Mythen (2004),4. Ericson and Doyle (2004),141.
[332] Beck (1999),32. Aradau and Van Munster (2007),93.
[333] Beck (2002),41. Aradau and Van Munster (2007),93. Cf. Clauset et al (2007).
[334] Beck (2002),41.
[335] Beck (1992),46. Vedby Rasmussen (2006),37.

remains unaffected.[336] Therefore, it is possible to control risks on a micro-level by choosing a particular preventive system, but aiming for universal safety and control is impossible.[337]

I side with Vedby Rasmussen, Adams and Beck in their way of risk as manageable without eliminating them all together. The perspective of this thesis is that scientific and technological development is a part of a constant innovative process, which makes it impossible to capture future risks to make precise guesses and estimations regarding their development. Managing cyber-space is a never-ending circle, every time one cyber-risk is somehow controlled; a new risk will emerge from the same control measures. Knowing that new risks will regularly arise in the realm of others, governments, groups and individuals need to retain resources to deal with the constant flow of new risks. Rasmussen claims that:

> “In the risk society you choose the risks you take rather than eliminate them all together”.[338]

This contradicts the idea that control is possible – and we need to accept and adjust to this as a part of the management process.

The foundation, for responding to cyber-risk in this thesis, is linked to the argument that risk in modernity is uncontrollable. It is only manageable because cyber-risks have a transboundary nature as risks:

> “[K]nows neither national boundaries nor a single global governance structure”.[339]

Therefore, I claim that the risk-management puts the traditional rules, practices and processes under pressure, and new forms of governance develop. Nodal governance provides the necessary flexible management structure to manage the continually developing risks. From my security perspective, it is possible to manage the unmanageable and maximise security through distinctive governance procedures imposed ad hoc. Cyber-risk governance originating from resilience and prevention – and management plans for detection and response, migration, and recovery are incorporated if a catastrophic event occurs.[340] There will always be ‘unknown unknowns’ where the unknown factor is high due to the technological development and

[336] Adams (1995) *Risk*,16, 52-53. Vedby Rasmussen (2006),35-36.
[337] Adams (1995),52-53. Vedby Rasmussen (2006),36.
[338] Vedby Rasmussen (2006),36.
[339] EC (2012b) ‘Tackling crime in our digital age’,2.
[340] Beck (1992),21.

the inconsistency in perceiving and interpreting cyber-risks worldwide. In a limited and defined area, it can be possible to control the area through governance procedures and practices developed (micro-level). However, on a macro scale, only globally accepted management processes can deal with the problem to the extent correct data is available.

3.8 Anticipatory Governance and Practices

Anticipatory governance is developed under the risk-management concept. Therefore, it includes all the parameters discussed above. Anticipatory governance encompasses actions beyond sound analytical capabilities and relevant empirical knowledge. This approach is based on distributed collection of social and epistemological capacities, which includes collective self-criticism, imagination, and the ability to learn from trials and failures.[341] The way in which cyber-security is conducted, includes a variety of management directions and techniques introduced in an attempt to manage the down pits in the technological development. I would call the governance form alternative because it is, in many aspects, pioneering and based on a high level of technical uncertainties, and there is no fact-sheet for managing the area. Moreover, all actors are improvising and testing different response techniques, which includes complicated management forms. This framework embeds knowledge, democracy, interactive policy-making, uncertainty, doubt and indeterminacy.[342] Anticipatory governance relates to the responses of constant transforming technological cyber-risks away from the production of reactionary and retrospective activities.[343] This requires a rethinking of governance and practices in a flexible regulatory system.[344]

My understanding of anticipatory governance is based on a particular way of analysing potential cyber-risks at an early stage; where framing and responding to risks need to be tailored to accommodate the significant features of risks. The acceleration of technologies and risks calls for a more sensitive approach to capture the faint signals about alternative risk characteristics that can identify possible problem areas early in the process, without being tied up to bureaucratic procedures and a command-and-control approach. The loosely founded nodal structure enables security actors to respond with greater flexibility and speed compared with traditional threat-based frameworks.[345]

[341] Barben et al (2007),992. Cf. Guston (2014) .
[342] Guston (2014),226.
[343] Barben et al (2007),992.
[344] Cf. Barben et al (2008). Anderson (2007). Quay (2010). Karinen and Guston, D. H. (2010). Ozdemir (2009). Gorman (2012).
[345] Fuerth (2011). Operationalizing anticipatory governance,33.

Fuerth correctly argues that anticipatory governance entails a complex system of institutions, rules and norms. I support Fuerth's argument, that these government types of responding to the risks by using foresight, networks, and feedbacks. The idea is to increase the capacity to respond to events early in the process.[346] Therefore, governance forms are developed to deal with the unexpected and the fragmented risks in different stages of the management process. Moreover, cyber-governance is organised in a way, where it will adjust rapidly to the interactions between policies and problems.[347]

I perceive the risk as manageable to the extent that it imagined and made known. However, the constant transformations of the techno-scientific risk patterns give little space for manoeuvring and developing sustainable structures. The problem of risk-based security is related to the way bureaucracies are procrustean in responding to new issues by forcing them into old concepts that are unfit to encompass them.[348] The technological challenges of managing cyber-space that we face are crosscutting because they simultaneously engage social, economic and political systems in multileveled security frameworks. As a result, measures and strategies are required to extend the horizon of awareness by looking into the future.[349] These are directed towards improving capacities to orchestrate both planning and action, which speed-up the process of detecting security errors and spread knowledge regarding computer technologies and management forms.[350] Within this framework, it is possible to introduce different steps to increase security, such as resilience, risk-management, threat–assessment and preparedness. Moreover, prevention, precaution and pre-emption are tools used under the anticipatory heading. To progress the understanding of cyber-security, and the different anticipatory techniques incorporated, I have designed a security-circle that progress from resilience to preparedness (figures 3 and 4).

3.8.1 Resilience and Preparedness

Cyber-security and governance is developed in a climate of uncertainty because of the constant technological changes and as a result, it is nearly impossible to predict future security directions. CI, CII and ICTs are deeply integrated into all aspects of life, which means that if a large-scale cyber-attack is carried out it will have unimaginative consequences. The terror attacks on 9/11 have intensified the use of risk-based

[346] Barben, et al (2007),993. Fuerth (2011),36. Guston (2014),226.
[347] Fuerth (2011),36.
[348] Fuerth (2011),33. Guston (2014),225.
[349] Fuerth (2011),31. Barben et al (2007),986.
[350] Fuerth (2011),31.

governance, recognising that the previous use of risk-management has serious flaws.[351] The ability to imagine future scenarios based on the technological development of computer science increase the success rate of risk-management. According to Coaffee and Rogers, the new security challenges in the aftermath of the events 9/11 had a dramatic effect. One of the consequences of the attacks was that they have brought imaginative techniques into the security framework which plays a significant part of cyber-security, where they can prompt responses to a variety of security risks.[352]

O'Malley claims that resilience is more to do with imagining increasingly uncertain and traumatic futures. This aims to create subjects that are capable of adapting and responding to situations of radical uncertainty.[353] Lentoz and Rose correctly point out that the growing scenario planning seeks to imagine different types of dangers in order to create a more resilient society.[354] Yet, it is important to remember that the concept of resilience does not take one specific form, nor is it possible to capture all risks in society. Walklate et al. have correctly highlighted the fact that resilience is not an objective condition, nor is it an absolute state, which individuals or communities can reach through cooperation. Instead, there are many types of resilience, which manifest themselves in a spectrum of different conditions, depending on the context.[355]

From my perspective, resilience and preparedness are the pre-condition or a response to failures in anticipatory governance. I would argue that to manage cyber-security, it is important to have a system of foresight to analyse alternative futures, which monitors prospective events, timely warnings of oncoming major events or technical developments, and alert policy-makers about potential consequences.[356] The nodal governance structure does not only comprehend prevention of risks, but it also advances security by using preparedness and resilience. Following on from O'Malley, I find that the way of seeing and anticipating future cyber-scenarios bares a close resemblance to science fiction, where technological innovations sound like impossible scenarios. Nevertheless, these scenarios could quickly become real, and the anticipatory

[351] O'Malley (2012),2.

[352] Coaffee and Rogers (2008) 'Rebordering the city for new security challenges,102. Guston (2014),226. O'Malley (2012),6. Cf. Grusin (2004) 'Premediation'. Taylor (2007) 'Global financial warriors'. Fagan (2001) 'The next wave of terror'. Dershowitz, (2006) Preemption: A Knife That Cuts Both Ways. Der Derian (2005) 'Imaging terror: logos, pathos and ethos'. 9/11 Commission (2004) *Final report of the National Commission on terrorist attacks upon the United States.* Aradau and van Munster (2007).

[353] O'Malley (2010). O'Malley (2012),6.

[354] Lentzos and Rose (2009),243. Brassett and Vaughan-Williams (2015),38.

[355] Walklate et al (2013),15. Walklate et al (2013b),12.

[356] Fuerth (2011),36.

framework creates a forum for testing actions that otherwise would be left in a threat-security reality, where the consequences of a failure to trace very weak risk-signals would be irrevocable.[357] Yet, this is not always possible to capture all cyber-risks. Aradau and van Munster state correctly that not everything can be predicated and systemised, and because of the high level of uncertainty about cyber-risks and future technological developments, everyone needs to expect the unexpected all the time.[358]

I find that the concept of resilience and preparedness takes a central position in the anticipatory risk-framework, and the inclusivity of the concept is based on a desire to developing plans, to manage the unimaginable, and to prepare for recovery and continuity after a catastrophic event (figure 3). My understanding of resilience and preparedness it linked to the ongoing process, which aims to decrease vulnerabilities in society. This is done by enhancing the resilient security framework that prevents possible cyber-scenario to unfold which would damage infrastructure and computer systems. It is in this context of living with risks that the discourses of resilience and preparedness have emerged, and these concepts are now seen as central components of the risk-management circle (figures 3, 4, 5 and 6).[359] This argument is supported by Walker and Cooper. Walker and Cooper argue that resilience is an approach to risk-management that forego the limits to predicative knowledge and incorporate the prevalence of the unexpected in order to absorb and accommodate future events in whatever forms they might take.[360] However, the obsession with future risks places the security actors and society permanently on the verge of disasters. Brassett and Vaughan-Williams capture the idea of resilience as a continuous activity that constantly changes as a result of its failures.[361] I support this idea in relation to cyber-security where the technological future is unpredictable and contains a large number of unknowns. Therefore, there needs to be incorporated barriers which prevent the risk from developing. However, I find it equally important to develop plans to ensure that CI, CII and ICTs also are operational after an attack. O'Malley also incorporates the circular approach by incorporating both the beginning and the end in his research. O'Malley

[357] Fuerth (2011),36.
[358] Aradau and van Munster (2012)
[359] Brassett and Vaughan-Williams (2015),34.
[360] Walker and Cooper (2011) ,146. Brassett and Vaughan-Williams (2015), 36, Norris et al (2008) 'Community resilience as a metaphor', 130.
[361] Brassett and Vague-Williams (2015),9. Dunn Cavelty et al (2015),9.

argues that resilience is related to technologies of preparedness as well as the actual process of coping with the catastrophically event.[362]

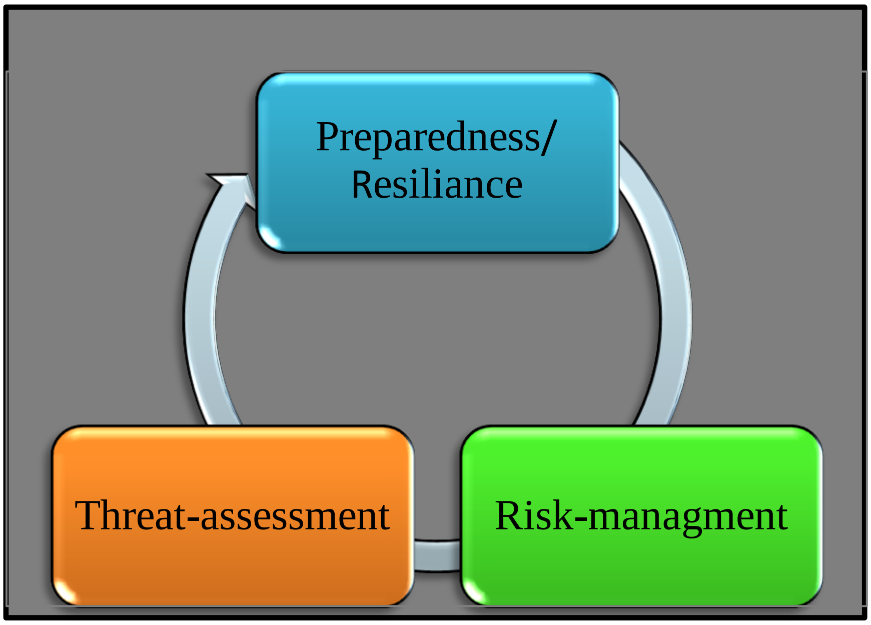


Figure 3 the security management process

The use of resilience in this thesis covers the techno-scientific nature of the Internet and cyber-space where it is required to minimise vulnerabilities of the everyday use of computer technologies. In this context, resilience is linked to disaster situations, i.e. terrorism, warfare, critical information infrastructure protection (CIIP), state failures, natural disasters and server breakdowns.[363] Lentzos and Rose argue that resilience includes a systematic, widespread, organisational, structural and personal strengthening of subjective and material arrangements. This is done to be able to anticipate and tolerate disturbances in complex worlds without collapse, to withstand shocks, and to rebuild.[364] Joseph has discussed the idea of including resilience in governance structures. In this context, governance includes an understanding of the interaction of political, social and economic resilience and human adaptability based on the complexity, i.e. self-organisation, functional diversity and non-linear ways of behaving.[365] The strategic level requires a rethinking of security structures in networked

[362] O'Malley (2010), 488.
[363] O'Malley (2012),10. Cf. Tombs and Whyte (2006) 'Work and Risk'. Wilkinson (2009) *Risk, vulnerability and everyday life*. Brand and Jax (2007) 'Focusing the meaning(s) of resilience',23.
[364] Lentzos and Rose (2009),243.
[365] Gunderson et al (2002) 'Resilience of large-scale resource systems',6, 8-12. Joseph (2013),2. Cf. Guston (2014). Cooper (2006) 'Pre-empting emergence'. Beck (1992). Erikson (1994) *A new species of trouble'*.

formations. A traditional inter-agency system provides only intermitted coordination of efforts among the different actors, and is therefore, unlikely to handle complex priorities alone.[366]

Reid argues that subjects that are capable of securing themselves are less likely to be considered a security threat, and therefore, they are not seen as a threat to states, businesses, groups or individuals.[367] I believe that even though states, businesses, groups and individuals are responsible for managing the growing risk of cyber-crime and cyber-attacks, it is clear that individuals are set on managing cyber-risks when they arise in everyday life. I have included Reid's argument in this thesis. I argue that cyber-security involves a number of different actors, including states, organisations, groups and individuals, and all of these actors have a role to play in order to create a more resilient society towards cyber-risks. From my point of view, enhancing resilience and preparing for possible attacks is a responsibility for everyone who has access to computer systems and technologies (section 5.5.2). Nevertheless, I support Mythen's argument that the more institutionalised security actors bear a greater collective responsibility to ensure a safe online environment and to uphold a functional infrastructure. The state, computer technology/Internet providers and various security actors have a shared responsibility to communicate the risks effectively to the public and to create functional governance forms. This would enable people to make decisions about appropriate behaviour and actions to enhance resilience against attacks, and prepare functional security solutions before and after an attack.[368]

3.8.2 Preparedness and Continuity

Holling argues that resilience determines the persistence of relationships within the system, created to absorb changes in different variables and parameters. Preparedness is placed at the end of the circle to manage the consequences of catastrophic events, and the concept can be defined as a form of planning for unpredictable catastrophic events. However, both O'Malley and Holling correctly claim that the aim of this kind of planning is not to prevent them, but rather manage their impact.[369] From my security perspective, the most important element in anticipatory governance is to increase resilience by manage the uncertainties and the vulnerabilities. I believe that in order to enhance resilience, the key element is to imagine unlikely situations and have plans

[366] Fuerth (2011),34.
[367] Reid (2012),74. Brassett and Vaughan-Williams (2015),34.
[368] Mythen (2015),45.
[369] O'Malley (2012),8. Holling (1973),23.

prepared to react to them. Preparedness covers a series of discourses, practices, technologies linked to the apparatus of security. Preparedness is, therefore, located under the resilience governance structure. This allows the system to withstand management failures based on an incomplete understanding, and it allows actors in resource's systems the opportunity to learn and change. In this case, resilience and preparedness progress through preventive procedures, such as contingency plans, risk assessment, exchange of information.

O'Malley states that preparedness is based on the creation of routines and resources for managing emergencies that are imaginable rather than accurately calculable.[370] The focus on preparedness derives from the notion that security management encompasses a broad range of organisations preparing for external threats and security risks. To govern the uncertainty, techniques beyond prevention have emerged, such as precaution, pre-emption, enactment and preparedness.[371] According to O'Malley, these techniques combine two features. Firstly, the imagination to project actions into the future and secondly, the use of an every-day calculus based on knowledge in order to identify potential hazards and/or opportunities to which they give rise.[372] Lentzos and Rose state that preparedness has obtained a new position beyond the traditional meaning of the word. It is impossible to capture all risks beforehand, and some remain unnoticed until the catastrophic event occurs. As a result, I incorporate preparedness in the ongoing security circle, as plans are required in all stages of the process (figure 3). From this perspective, preparedness covers all aspects of prevention, protection, first response capacity, prosecution, surveillance, research capabilities, responses and recovery. These areas also include taking steps to minimise the threats before it develops further.[373] In this context, Lakoff notices that precautions are increasingly linked to preparedness as a management technique for catastrophic future probabilities which use the operational criteria of response – rather than total avoidance.[374]

3.8.3 Anticipatory Management Techniques

As well as resilience and preparedness, prevention, precaution, and pre-emption are management techniques which are equally incorporated in anticipatory governance (figure 3). To achieve insight into cyber-security, I consider these governance

[370] O'Malley (2010),489.
[371] O'Malley (2012),6.
[372] O'Malley (2012),5-6.
[373] Lentzos and Rose (2009),235. EC (2007a) 'Green paper on bio-preparedness',3.
[374] Lakoff (2006) 'Techniques of preparedness',9. Aradau and Van Munster (2008),30.

techniques and perspectives equally important to understand governance strategies as they open up for the use of proactive responses rather than using the traditional threat-based form of governance. Moreover, it highlights the complexity of security measures and the use of nodal governance to respond to the different types of risk, which can be perceived differently depending on the underlying relations. I think that in order to anticipate and take advances of the transformative capacities of computer science, the dangerous side effects need to be imagined, calculated and responded too. However, the pace of the innovations makes it impossible to calculate the dangers and, as a result, it is necessary to incorporate preventive and precautionary management steps in governance and practices on an early stage. Management techniques are part of the same logic as resilience and preparedness. These are tools for sorting through certainties and uncertainties in order to develop responses on a case-by-case basis based on future-oriented perceptions, cross-impact estimation and new ways of technology assessment.[375]

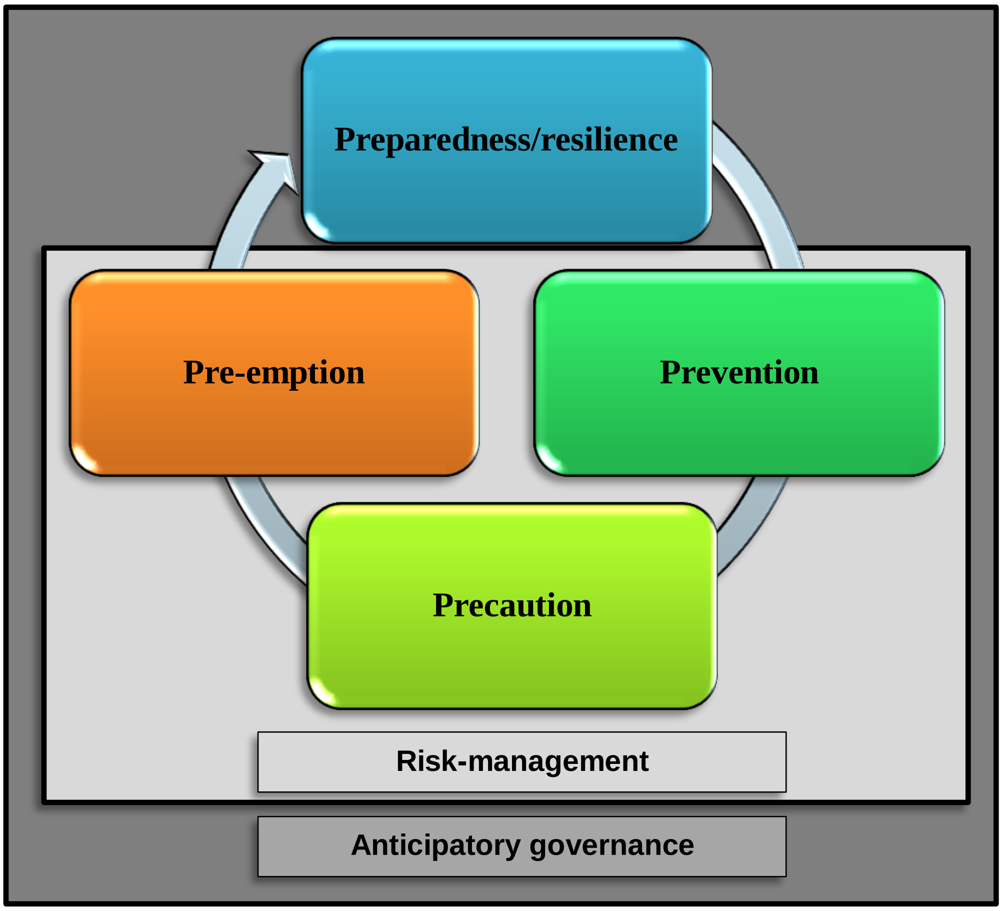


Figure 4 resilience and preparedness in the risk-management circle

[375] Barben et al (2007),986.

Prevention is used to stop or minimise the possibility of known events occurring. If the prevention fails due to uncertain knowledge, the precautionary principle is used to avoid the event developing further until the problem is clarified. The preventive framework focuses less on gathering evidence, prosecution, conviction and subsequent punishment, but it is applicable towards targeting and managing the threat through disruption, restriction and the incapacitation of risky individuals or groups.[376] For example, cyber-security is considered a high-level security risk because it is possible that an attack can happen again, and it is uncertain how and when an attack will be carried out. Using preventive techniques is it possible to prevent actions against expected targets based on information from previous attacks, i.e. types of malware against CI, CII and ICTs. Under these circumstances, it is about minimising the gap in security by creating barriers against attacks. [377]

I consider precaution to be part of the same logic, but the lack of knowledge distinguishes it from prevention. Precaution is defined by the safety first terminology where there is no scientific certainty. Yet, the lack of knowledge cannot be used as a reason for postponing cost-effective measures to prevent potential risks from transforming into threats.[378] The rationale behind the concept of taking precaution against a risk derives from the proverb 'better safe than sorry'.[379] In the security industry, the use of the principle derives from the assumption that:

> "[W]aiting for proof will mean waiting until it is too late to avert catastrophe".[380]

Aradau and van Munster claim that the precautionary principle requires that regulatory actions is not based on existing knowledge, but it is based on what we do not know.[381] As Hebenton and Seddon correctly argue, the precautionary logic confronts the limits of science at two points. Firstly, there are areas where science can no longer produce

[376] McCulloch and Pickering (2009),4. Cf. Collins (2000) 'Preemptive prevention',224-225. Fisher (2001) 'Is the precautionary principle justifiable?'318. Stern and Wiener (2006) 'Precaution against terrorism',404. Coaffee (2006) 'From counterterrorism to resilience',395. Sandin (1999) 'Dimensions of the precautionary principle',892. Sandin (2004) 'The precautionary principle and the concept of precaution',462.

[377] Sandin (1999),892. Cf. Goldsmith (2008) 'The Governance of Terror'.

[378] UNEP (1992) 'Rio declaration, Principle 15',2. Morris (2000) 'Defining the precautionary principle',5. Sunstein (2003) 'Beyond the precautionary principle',1012. Fisher (2001),318. UNEP (1992),2. O'Riordan and Jordan (1995) 'The precautionary principle in contemporary environmental politics',193. Sunstein (2003) 'Beyond the Precautionary Principle', 1006. Wingspread Conference (1998) 'Wingspread statement on the precautionary principle'

[379] Sandin (2004),462. *In the precautionary terminology, it signifies "nothing is safe, as long as it has not been proven harmless".* Beck (2006) 'Living in the World Risk Society',337.

[380] Stern and Wiener (2006),397. Cf. Sandin (2004), Sandin (1999), Freestone and Hey (1996) 'Origins and development of the precautionary principle'.

[381] Aradau and Van Munster (2007),102.

useful information about risk. Secondly, where such applied science in itself creates new uncertainties with possible worst-case outcomes.[382]

Pre-emption follows the precautionary logic.[383] In this context, Hebenton and Seddon illustrates how closely related pre-emption and precaution are by stating that pre-emption entails a form of radical precaution.[384] Zedner argues that the pre-emption stands temporally prior to prevention of immediate harms as it seeks to intervene when the risk is unspecified, uncertain and beyond view.[385] In relation to security, there is an increased trend towards using pre-emption, mainly to prevent grave harm caused by security problems and war, justified by the right to self-defence. This is in situations where the threat of attack does not leave a moment for deliberation.[386]

In security strategies, the use of the logic of precaution is central, not the principle in itself. Nevertheless, I find that the precautionary logic holds a significant position in cyber-security as technologies evolve so fast that there is not enough scientific knowledge available. Beck and Weigart et al. argue that promoting a catastrophic interpretation that justifies the use of the logic of precaution as an ‘act-and-learn’ rather than a ‘wait-and-see’ approach.[387] If the harm is caused, it can be irreversible, difficult or expensive to restore.[388]

[382] Hebenton and Seddon (2009),351.

[383] Aradau and Van Munster (2007),103.

[384] Hebenton and Seddon (2009),345.

[385] Zedner (2007) ‘Seeking security by eroding rights’,259. Zedner (2009),85. Litwak (2003) ‘The new calculus of pre-emption’,54.

[386] Zedalis (2005) ‘Circumstances justifying pre-emptive self-defence’,214. Waltzer (1977),74. Cf. Sofaer (2003) ‘On the necessity of pre-emption’. Zedner (2007), Litwak (2003).

[387] De Goede and Randalls (2009) ‘Precaution, preemption’,863. Sunstein (2008) ‘Irreversibility’,1.

[388] Sunstein (2008),3.

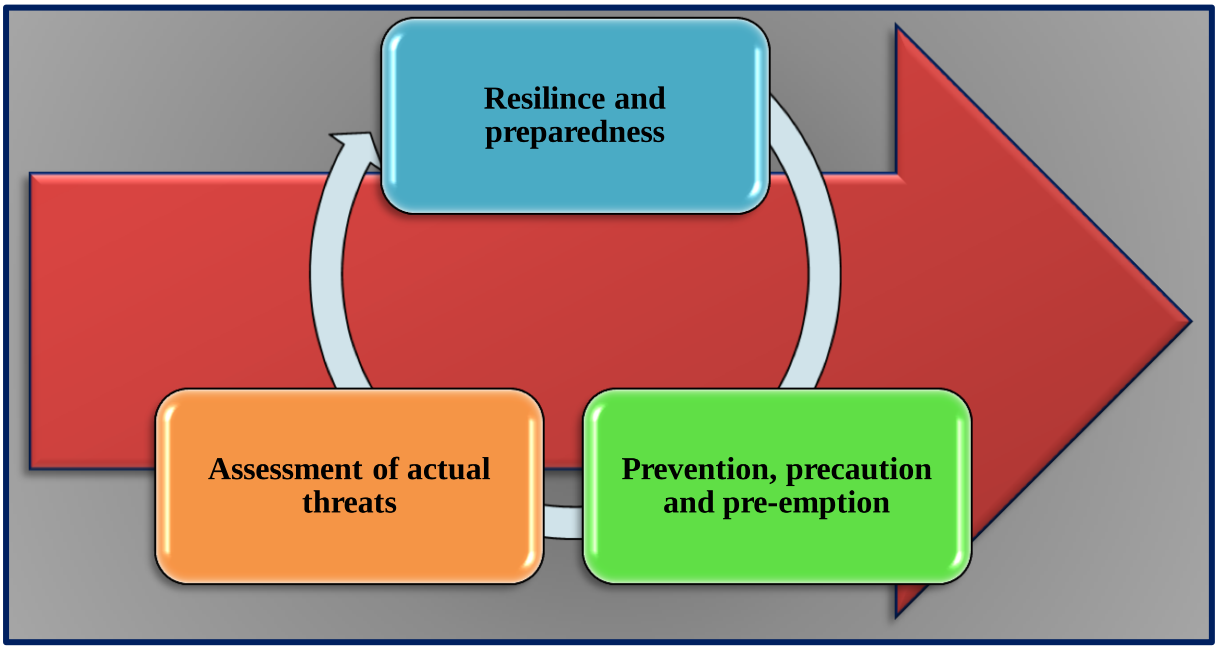

Resilince and preparedness
Assessment of actual threats
Prevention, precaution and pre-emption

Figure 5 the continuous circular processes of risk-security management

Risk-based security strategies are regularly reviewed and restructured to reflect the changes in risks. Overall, the security processes can be illustrated as follows; there is a circular process, which continually reinvents the anticipatory governance forms depending on the success rate of the measures imposed (chapters 5 and 6). However, it is also a continuing process, as new risks arise as soon as one is managed.

3.8.4 Risk-based and Threat-based Security Management

Risk-based security strategies change the focus by constantly attempting to interrupt the possible conditions of harm imposed by future risk, rather than removing threats (chapters 2 and 3).[389] The difference between the construction of risk and threat can be found in the time scale as they are performed at different stages of the security process (figure 5 and 6). I have created a circular model to cover both risk and threat in the same process depending on the level of uncertainty, which separates risk-management and threat-assessment. This is done, as I consider anticipatory governance relevant to manage risk before and after a catastrophic event. Before the event, proaction is evoked to build preventive obstacles to stop the risk from mutating into threats. After the event, proaction has relevance by imagining new worst-case scenarios and developing plans to minimise future consequences, i.e. contingency and mitigation plans. These programs will not prevent attacks from happening, but if they do occur, any negative impact is

[389] Corry (2010) ‘Securitization and ‘riskiziation,14.

potentially reduced. This is highly relevant in cyber-security, where all computer users have a responsibility to secure their network, but because of the technological development, there will be gaps in the security structure.

Figure 6 below illustrates anticipatory risk-governance in an ongoing process involving both risk and threat politics. It is obvious that the construction of these two security types differs in the construction and the actual management of the security problem. Proactive planning can never be absolute, nor can it be sufficiently comprehensive to include all consequences. Hence, it is necessary to imagine worst-case scenarios to develop security barriers that can minimise the consequences and ensure recovery. In relation to cyber-security, there is a requirement for a strong imagination in order to predict future technological development and possible types of attacks. Therefore, anticipatory governance forms are linked to their ability to prevent a particular situation and to develop recovery plans to maintain essential functions, despite events that might cause dramatic changes or disruptions.[390] This overlaps to some degree with threat-based security, and I claim that by mutating into an actual event, the risk has transformed into a threat. Therefore, if the risks develop into an actual threat or worse, anticipatory risk-management is no longer used; instead, a deterrence mechanism is enforced to control the event. However, this does not stop the ongoing process, as a new risk can grow out of the actual episode that calls for instant management.

[390] Corry (2010),14.

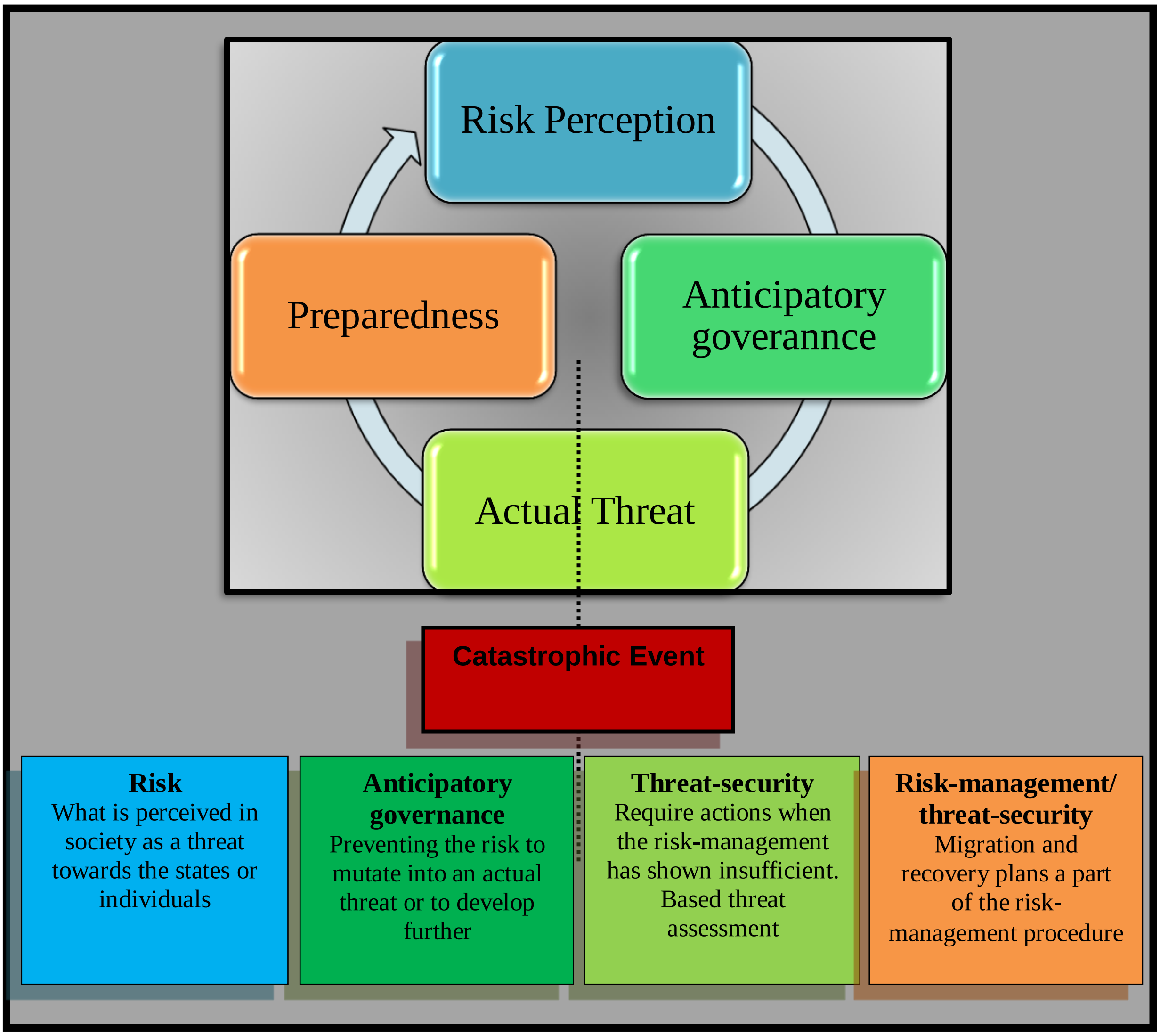

Risk Perception
Anticipatory governannce
Actual Threat
Preparedness
Catastrophic Event
Risk
What is perceived in society as a threat towards the states or individuals
Anticipatory governance
Preventing the risk to mutate into an actual threat or to develop further
Threat-security
Require actions when the risk-management has shown insufficient. Based threat assessment
Risk-management/ threat-security
Migration and recovery plans a part of the risk-management procedure

Figure 6 the ongoing security governance circle

3.9 Conclusion

The review, in this chapter, enables me to precede with my research objectives by creating a foundation for discussing cyber-security and governance forms. In the nodal framework, it is possible expand the security networks to encompass new security alliances and networks, such as public-private cooperation, promotion of small enterprises, introduction of strategic frameworks, and other public information products, which are needed to manage the constant transforming cyber-risks. This empowers communities and practitioners to collaborate more efficiently. I chose to analyse cyber-security strategies through the lenses of nodal and anticipatory governance. This hybrid construction is based on cooperation between numerous security actors and constantly changing formation depending on ad hoc management, where solutions are designed for a specific risk-related problems or tasks. I have promoted the viewpoint that we live, not only in a risk society, but also in a networked individual society, which requires a nodal construction to encompass the variety of cyber-risks. This argument brings forward the fact that the process of individualisation takes place, and cyber-security strategies include this. Interconnected networks include different individual actors, such as states, groups, businesses, individuals. In this context, I believe that collective organisation forms are replaced by new, more active and flexible security structures, in which a number of actors are brought together in an interconnected system.[391]

I argue that because of the increased focus on risk, measures, and governance take precedence to manage possible risk areas; anticipatory governance creates space for preventive, precautionary and pre-emptive measures. Under this umbrella formation, I acquire analytical insight into the framing and management of cyber-security. In this thesis, I argue that cyber-security problems are linked to globalisation, the variety of risks in and from cyber-space, the rapid technological development and the futuristic approach. However, models developed to deal with real-world crime often structure the main problem with managing cyber-related crimes and other cyber-mediated dangers, preventive measures and law enforcement operations. This is done, despite the fact that cyber-attacks, in all its forms, do not share the same characteristics, and therefore, the procedures cannot deal effectively with cyber-security. It is essential for the governance processes that alternative solutions are sought, and both objective and subjective interpretations are involved in the construction of the dangers (chapters 1 and 2). The high level of uncertainty that surrounds the application of the concept requires that earlier actions are taken compared with the threat assessment. Anticipatory governance forms are used to enhance resilience and preparedness, and these cover three different areas, i.e. prevention, precaution and pre-emption. Risk governance is a continuing process because it is believed that risks cannot be controlled. However, this process contains the paradox that the management procedures used quickly can produce more risks in a never-ending process. This is illustrated by the figures I have designed to enhance the understanding of the current security-circle deployed to manage cyber-security. Risk-management requires different techniques and knowledge in order to be involved in the management structure and this creates an intellectual and substantive challenge to security actors (chapter 5 and 6).

[391] Joseph (2013) ‘Resilience in the UK and French security strategy’,3, 6.

4 Two Security Schools and Synthesising the Theoretical Foundation

4.1 Introduction

This chapter introduces two security schools used to increase the understanding of cyber-security following the theoretical foundation of nodal and anticipatory governance. As a result, this chapter addresses the research objectives central to establishing cyber-security in contemporary policies. Two security schools, the Copenhagen School and the Paris School, represent different ways of seeing safety procedures, practices and contesting management forms, i.e. exceptionalism vs. regular processes, threat vs. risk, and state vs. individual security. For the purposes of this thesis, the two key schools of thought are central to my argument. While the schools represent only two of a number of approaches within critical security studies, they have been selected because they both provide an ample body of research and their critical perspectives. Additionally, they have also been chosen because much of their research involves wrestling with some of the same questions contained in this thesis. However, the Copenhagen School and the Paris School need not be subsumed into one identity. Thus, it is important to distinguish them by reference to what they say about security, how they say it and why it matters. A review of these two security directions provides an understanding of their role to define anticipatory governance forms and practices in the European security framework. By choosing these two security strategies, I do not indicate that other security theories and approaches are unimportant, i.e. critical security studies, critical constructivism, feminist security studies, human security, peace research, post-colonial security studies, post-structural security studies, strategic studies, neo-realism, etc. They, however, target different aspects of the security dilemma, which falls outside the scope of this research (section 1.4).[392]

I will discuss two areas in this chapter. Firstly, I will discuss the perspectives of the two security schools in order to outline their underlying structures and usefulness for analysing cyber-security. Secondly, the objective of this chapter is to synthesise a theoretical framework for the substantive analysis of cyber-security by drawing on the perspectives on risk and security discussed in the preceding chapter. This chapter connects the theoretical and substantive parts of the thesis. These case studies (cyber-security and cyber-terrorism), draw out and adapt key ideas from the theoretical material discussed in chapters 3 and 4. Therefore, I highlight three critical areas, which

[392] Buzan and Hansen (2009),36-37, 187ff.

develop the framework for the substantive analysis. These three areas are central to the discussion in part two which covers security actors and the development of rules, practices and processes. Finally, this chapter will outline the empirical methodology for the substantive analysis where I outline the process of identifying the research area, collecting data and analysing documents.

4.2 Two Schools in Security: The Copenhagen School and the Paris School

The way in which cyber-security is framed and managed, contains a mixture of different approaches and perspectives. These approaches and perspectives have direct links to the previous security paradigm, where exceptional policies brought military means and methods into the civil society (section 2.4.1).[393] However, anticipatory risk-management has developed parallel to the military model of exceptionalism (section 2.4.2). The aim of this thesis is to build on the nodal governance foundation, and these two security perspectives provide insight into how cyber-security is understood and managed by the different actors. Moreover, I argue that the security concept shows how multileveled cooperation is developed in the security area that lacks a functional definition and analytical model for governance. I suggest that the problem is related to the global networked system, where there is a considerable lack of harmonisation between the various jurisdictions, law enforcement systems and interactions between security actors involved. By having security actors from different sectors on the horizontal and vertical level, there is a problem with the allocation of power and accountability. However, in cyber-security a new logic has emerged. Online safety is not only about enhancing security; it is about anticipating the future to be able to adopt measures and policies, which will increase resilience and preparedness towards potential targets (section 3.7.1).[394]

From my security perspective, the two schools do not give a clear-cut solution to these problems. However, they offer a critical approach to security, which can be transferred to cyber-security in order to improve understanding of this security dimension. The security perspectives of the Copenhagen School have been linked to the exceptional policies used during the ‘War on Terror’, where their academics have been critical

[393] Cf. Neal (2012a) ‘Normalization and legislative exceptionalism’. Aradau and van Munster (2009),686-701.
[394] Dunn Cavelty (2008),137.

towards the management methods.[395] Although risk-management strategies have obtained a prominent position, securitization is still considered essential to the issue of security, if/when risks mutate into actual threats that require exceptional policies.[396] I use the state-centric approach of Copenhagen School's securitization to define the boundaries of the state as a security actor in opposition to the individualistic approach of the Paris School.[397] Nevertheless, two scholars, Nissenbaum, and Hansen, have applied securitization to cyber-security and this new approach will be discussed throughout the thesis.[398] Compared to the Copenhagen School, the work of the Paris School is harder to define. This security approach is centred on interactions between internal and external security on all layers of society.[399] I think that the Paris School's perspective on governmentality is useful for understanding governance and practice, as the school critical analyses interactions between security professionals and experts in smaller groups.

4.3 Broadening and Deepening the Security Agenda

The definition of threat made by Ullman (section 2.2) marks the starting point for changes in the perception of security and what can be threatened (state and non-state security). The Copenhagen School broadened the security agenda, whereas the Paris School belongs to the group which argues that security has a deeper significance. I would argue that the differences between the two schools highlights that there is something about conceptual breadth and depth at stake in both these schools. Academics of the Copenhagen School have been highly critical of the way security has been conducted in the past. Therefore, this school has successfully argued for a broadening of the security agenda due to the changing realities of the world (section 2.4).[400] From their security understanding, security no longer holds a single fixed meaning. For them, the concept is changeable due to political and societal changes that open up a wider application of security.[401] This change in security signifies that it is

[395] *The essence of the work by CS is built around three main ideas, which are securitization, sectors, and regional security complexes.* Wæver (2004) 'Aberystwyth, Paris, Copenhagen',8. Buzan et al. (1998). Cf. Emmers (2010) 'Securitization', 139. Salter (2008b) 'Securitization and desecuritization',324-325.

[396] Buzan et al (1998). Cf. Aradau and van Munster (2009),686-701.

[397] Buzan et al (1998). Cf. McDonald (2008). Securitization and the construction of security,563-587. Stritzel (2007). Towards a theory of securitization',357-383. C.A.S.E. Collective (2006),443-487. Taureck (2006) 'Securitization theory and securitization studies,53-61.

[398] Hansen and Nissenbaum (2009).

[399] Bigo (2008b) 'International political sociology', 126. Van Munster (2007) 'Review essay: Security on a shoestring', 236.

[400] Sheehan (2005),47. Buzan et al (1998),8,

[401] Sheehan (2005),48. Buzan (1991b) 'Is international security possible,42.

essentially a contested concept, which follows political and societal developments.[402] However, this approach limits the areas that can be securitized by only linking it to military, political, economic, societal and environmental sectors (cyber-security considered as the sixth sector).[403] As highlighted in the historical analysis in the previous chapter, the development of security spans from a military concept of a broader perspective. The purpose, of selecting these areas, is to reduce the complexity of security in order to facilitate analysis.[404] The background for this theoretical perspective is to explore the logic of security itself to find out what differentiates security and the process of securitization from that which is merely political.[405] The effect of broadening the security agenda is that states are enabled to use emergency measures to address a range of security problems by overcoming the usual barriers of actions.[406] From this point of view, these sectors are defined as:

> "[T]he military sector is about relationships of forceful coercion; the political sector is about relationships of authority, governing status, and recognition; the economic sector is about relationships of trade, production, and finance; the societal sector is about relationships of collective identity; and the environmental sector is about relationships between human activities and the planetary biosphere".[407]

A deepening of the security agenda has developed parallel to the broadening approach. Booth has contested Paris' interpretation of the deepening security agenda, where Paris has defined it as:

> "By deepening, I mean that the field is now more willing to consider the security of individuals and groups, rather than to focus narrowly on external threats to the state".[408]

Booth argues that deepening the security agenda is not about looking at state level, group level, individual level, etc.[409] Instead, deepening the security agenda investigates security policies by tracing them back their political assumptions and thereby, bringing security studies into the realm of politics.[410] As a result, this security direction is about the processes and practices developed, and these can constitute a threat to itself. By

[402] Bigo (2008b),120.
[403] Wæver (2004),8.
[404] Buzan et al. (1998),8.
[405] Buzan et al. (1998),4-5.
[406] Sheehan (2005),56. Buzan et al. (1998),25.
[407] Buzan et al. (1998),7.
[408] Booth (2007),157. Paris (2001),97.
[409] Booth (2007),157.
[410] Booth (2007),155.

deepening the security agenda, these processes are regularly reviewed and reinvented to capture all internal dangers within a constant changing security environment.[411]

The deepened agenda abolishes the external-internal dimension because security is not necessarily related to external threats:

> "Constructing 'threats' is part of constructing the 'other'; an identity imbued with characteristics we like to think are the opposite of our own. Rather than looking 'out there', we should concern ourselves with the problems and threats we cause".[412]

Booth has argued that security is not only about broadening the security agenda by extending the logic of security to new sectors. Just as with nodal governance, I find that parallel to the state, other security actors' practices, and procedures can be necessary beyond military, political, economics, societal and environmental sectors. Similar to national security and the integrity of the state, academics of the Paris School claim that security also concerns the identity and culture of particular societies, local communities or religions. In this context, all of these different levels are considered equally important because security cannot be limited to the geographical space.[413]

By deepening the security agenda, it is important to look at the heterogeneous structure rather than the homogeneity of the state – and this is significant in cyber-security where a number of different security actors are involved.[414] Objects of danger often play an important role in everyday life because they open the possibility that they could become a threat. Cities, drugs, planes, cars, mobile phones, databases and shopping malls are all viewed as useful objects or parts of daily routines, but they can be transformed into security dangers.[415] I would argue that the problems of executing cyber-security relates to the increasing use of critical infrastructure (CI), critical information infrastructure (CII), and information computer technologies (ICTs) in everyday life. As a result, every activity in cyber-space can contribute a possible risk to the users, i.e. groups and individuals. It is these different perspectives that separate the two schools, with the Copenhagen School focusing on survival, while the perspective of the Paris School centres on every-day practices concerning (in)security, i.e. fear of crime, poverty, illness, etc.[416]

[411] Booth (1997) 'Security and self',111. Sheehan (2005),58.
[412] Terriff et al. (1999),22.
[413] Bigo (2008b),120.
[414] Bigo (2008b),125.
[415] Bigo (2008b),125.
[416] Bigo (2008b),118.

4.4 The Copenhagen School on Peace and Conflict

Securitization was introduced after the Cold War, and this approach has had a significant impact on the security agenda and the interpretation of security, i.e. military and non-military issues. In relation to cyber-security, it falls short of engaging with the nodal-networked formation when it is interpreted in its original form. However, in the following sections of this chapter, I will outline the fundamental elements of the Copenhagen School's security perspective, which is useful for understanding the extended cyber-security version of securitization developed by Nissenbaum and Hansen (section 4.5).

As stated in chapter 2, security is defined by the Copenhagen School as a matter of survival, which can justify the use of extraordinary measures.[417] They provide an analytical framework for describing the processes involved in threat assessment and security moves (securitization).[418] Securitization are used when normal security processes fails to deal with the threat, and this can be a dangerous way which opens for exceptional politics.[419] Securitization is defined as:

> "[T]he move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics".[420]

This is echoed in Tony Blair's famous speech after the 7/7, terrorist attack in London (2005), where he said:

> "Let there be no doubt. The rules of the game are changing".[421]

Without any doubt, the game did change, and the changes did have an impact when the securitization move became the norm rather than the exception. In the current security agenda, I have found that there is a trend towards labelling an increasing number of issues as threats. This has opened up the security agenda beyond the original intention of the Copenhagen School.[422] The three-step process described in securitization has been predominantly in the 'War on Terror' and other declared wars, based on a particular militant rhetoric, i.e. the 'War on Drugs',[423] the 'War on Transnational/ National Crime',[424] the 'War on Cancer',[425] and the 'War on Poverty'.[426] Moreover,

[417] Buzan et al (1998),21.
[418] Wæver (2011) 'Politics, security, theory',692.
[419] Buzan et al. (1998),29, Floyd (2007),328. Booth (2007),165.
[420] Buzan et al. (1998),23.
[421] Walker (2007) 'The treatment of foreign terror suspects',427.
[422] *Originally, securitization was seen as a process applicable to issues, which is unable to be managed within the normal politicized area.* Buzan et al. (1998),23-24.
[423] McDonald (2008b),565. Simon (2008) 'Choosing our wars',88. Giraldo and Trinkunas (2010) 'Transnational crime',441-443.
[424] McDonald (2008b),565. Simon (2008),87-88.

immigrants and asylum-seekers are perceived as a threat to the sovereignty and the identity of national states (without calling it 'War on Immigration').[427] Burnett and Whyte highlight this:

> "The war on terror then, is rather similar to wars on crime, for although the problem is not constructed as a localised one, there is a similar tendency: to impose a set of common characteristics upon an enemy that enable it to be known".[428]

In the last decade, there has been a generalisation of security topics, which are securitized. The increase use of securitization is a dangerous route, as the increased application of securitization can water down the idea of exceptionalism. There is a danger of abusing securitization by legitimately empowering the role of the military or social security forces in civilian activities.[429] Following securitization, decision-makers can impose legislation that otherwise would have been rejected as breaching democratic values, fundamental freedom, and human rights (changing rules).[430] This is a slippery slope when the use of securitization procedures, becomes the norm rather than the exception. This process can be used to restrict civil liberties, impose military law, limit the impact of individual political institutions or detain political opponents and suspected terrorists without trial.[431]

4.4.1 Exceptionalism and the State-centric Approach

The Copenhagen School's security perspective is based on exceptionalism, in the sense that securitization is a stronger example of the politicisation, which can be used in particular situations of immediate danger.[432] The use of exceptionalism derives from Schmitt's theory of exceptional policies. He has argued that the exception can best be defined as a case of extreme peril where an issue is considered to be a danger to the existence of the state. However, it cannot be circumscribed factually and made to conform to a preformed law because the precise details of an emergency cannot be anticipated. Additionally, it cannot be precisely categorised by what may take place,

[425] Simon (2008),81.
[426] Simon (2008),79.
[427] McDonald (2008b),567.
[428] Burnett and Whyte (2005),6.
[429] Emmers (2010),142. Cf. Caballero-Anthony et al (2006) *Non-traditional security in Asia.*
[430] Buzan et al. (1998),23.
[431] Emmers (2010),142.
[432] Sheehan (2005),53. Cf. Buzan et al. (1998),23. Buzan and Hansen (2009),214. Emmers (2010),139. Wæver (2004),8.

especially when it is truly a matter of an extreme emergency and how this can be eliminated.[433]

I would argue that the problem is linked to the fact that exceptional measures tend to become the norm. Agamben argues that the declared state of exceptions has been replaced by an unprecedented generalisation of the model of security, which becomes the usual techniques of government.[434] Neal supports this argument. He links exceptionalism with securitization, stating that the security approach problematises the object of exceptionalism by theorising the way that events and situations are named and acknowledged as exceptional.[435] It is the practical use of securitization, which creates problems when exceptionalism is being misused. The Copenhagen School's approach is an attempt to understand what is happening in the world, not to develop a set of guidelines of what ought to happen. The term security establishes priorities for action and legitimates an enhanced use of exceptional measures.[436] Placing threat management outside the normal democratic processes gives the security actors a sphere to act within, and the principle can be applied in a wider framework hidden behind secretive practices and structures.[437]

Traditionally, the referent object has been protected by the state because this has been the only actor capable of securing the territory and its interests. Thus, it has the legitimacy to decide what constitutes an actual threat to a given object by determining that:

> "[I]t has to survive. Therefore, it is necessary to…".[438]

The traditional approach is that security is linked to the state:

> "[S]ecurity, by definition, is and should be about the state, and the state is and should be about security, with the emphasis on military and political security".[439]

Although the Copenhagen School attempts to circumvent this argument, they fail to make a strong distinction. The Copenhagen School claims that they have constructed a wider conceptual net, which goes beyond the traditional state-centric approach by

[433] Schmitt (1985) *Political theory*,6. Neal (2010) 'Exceptionalism and the politics of counter-terrorism',70.
[434] Agamben (2005) 'State of exception',87. Ericson (2008),58. Ericson (2007b),6. Ericson (2007a),388.
[435] Neal (2010),4.
[436] Sheehan (2005),52.
[437] Ericson (2008),57
[438] Buzan et al. (1998),36.
[439] Buzan et al. (1998),37.

allowing other security referents into the framework.[440] This argument is contradictory to the practical application of securitization. Booth states that securitization is too distant to real people, and it wrongly makes a strong link between security and survival, Moreover, Booth has criticised the state-centric approach. He rightly claims that the theory is:

> “[S]tate-centric, elite-centric, discourse-oriented, conservative, politically passive, and neither progressive nor radical”.[441]

Despite the school include other security actors in the reinvented approach (section 4.5); the Copenhagen School still places the state central to the speech act and securitization. The main argument of the Copenhagen School is that the state is the only one who has legitimate political power to impose a wider form of security.[442] The school has explained this limitation by using an example of economic security, where companies are considered as natural limited collective units. However, due to their nature, these businesses rarely have a strong claim to the right to survival compared to the state. If the survival of the company, business, etc. is threatened, these entities will not be able to legitimise actions beyond the ordinary legal rules.[443] I do not believe that this state-centric approach is applicable to the networked formation implemented in cyber-security, where cooperation transnational and cross-sectoral are central to the way risk is framed and managed through anticipatory governance. However, I believe that it is too early to reject the security approach, as there are situations where the risks are not managed correctly, and therefore, they develop into actual threats (section 3.7.3). This development can threaten the survival of a given referent object, and therefore, it can be necessary to let the security actor, state or individual, take the necessary steps to stop it from becoming a catastrophe.

4.4.2 The Speech-act, Securitization, and Desecuritization

Deeply rooted in the securitization theory is the use of a speech-act, which the Copenhagen academics consider to be the starting point of a three step process, i.e. speech-act, securitization, desecuritization.[444] Through a successful speech-act, the

[440] Buzan et al. (1998),36.
[441] Buzan and Hansen (2009),215. Neal (2010),108. Booth (2007),166. McDonald (2008b),579.
[442] Buzan et al. (1998),37. McDonald (2008b),574.
[443] Buzan et al. (1998),38.
[444] Emmers (2010),139.

security actor gets legitimacy from an audience to securitize an issue.[445] This is done in order to convince a relevant audience that a referent object is existentially threatened, and to generate a security move.[446] As a result, the political establishment accepts a security problem as being an actual and existential threat.[447] It is necessary to obtain this legitimacy, because the security move abandons standard rules or procedures that characterise democracy, i.e. public participation, openness, transparency, accountability and predictability. The securitization move follows an internal grammar between the speaker-audience. It can be outlined differently within the professional team and in front of an audience. However, the audience is not necessarily the public, but can be a group of bureaucrats, consultants, parliamentarians or officials, that must be convinced that this move is appropriate to manage the threat.[448] From my own security understanding, this process is clearly manipulative because it is solely linked to the construction of security issues, the rhetoric used - and how the speech-act is performed. It is based on the actors' intentions, regardless of the power of the state, to convene what the actor wants to be done, what the actor is prepared to do, and how to act if the speech-act is unsuccessful.[449] The whole process can be premeditated using a chosen audience, and pitched in a particular way in which the favoured audience will approve.[450]

When an emergency situation is confined, the last step can be enabled, i.e. desecuritization. Desecuritization can be described as the optimal long-perspective option, which can be moved out of the threat-defence sequence and into the ordinary public sphere when the security issue no longer constitute a threat.[451] Firstly, the unstable situation has to be stabilised. Secondly, the measure must be moved from the emergency sphere into the ordinary public area.[452] Unfortunately, this attitude towards desecuritization has changed worldwide during the last security paradigm to reflect the stance, 'the more security, the better'.[453] Yet, this underlines the critical perspective of the Copenhagen School:

> "[N]ational security should not be idealized. It works to silence opposition and has given power holders many opportunities to exploit "threats" for domestic

[445] Emmers (2010),141. McDonald (2008b),566, 579. Floyd (2007),329. McDonald (2008b),572-573. Pram Gad and Lund Petersen (2011) 'Concepts of politics in securitization studies',318. Buzan and Hansen (2009),215. Neal (2010),108. Booth (2007),166.

[446] Emmers (2010),139. Buzan et al. (1998),33-34.

[447] Sheehan (2005),53.

[448] Salter (2008b),327-328.

[449] Salter (2008b),327.

[450] Salter (2008b),328.

[451] Buzan et al. (1998),29.

[452] Buzan et al. (1998),29.

[453] Buzan et al. (1998),29.

> purposes, to claim a right to handle something with less democratic control and constraint. Our belief, therefore, is not "the more security, the better". Basically, politics should be seen as a negative, as a failure to deal with issues as normal politics".[454]

During the 'War on Terror', a number of problems have been managed using exceptional measures rather than the politicised processes.[455] Consequently, I find that desecuritization is less likely to happen, and the violation of democratic procedures increases when the emergency is upheld. It is not the only problem. Tsoukala has argued that these emergency rules tend to become a part of the ordinary model of governance. Security measures are also likely to be interpreted to cover other less severe security risks. The security measures become more entwined with the legal system than intended, and therefore, they become harder to remove from the system through desecuritization.[456] Moreover, it is hard to identify when a desecuritization can begin.[457] I believe that the problem is not linked to the binary difference between normal times and exceptional times. Instead, it is based on the political and legal processes, which are entailed by exceptions and emergency powers that have blurred that distinction.[458] Additionally, I also think that it is problematic that cyber-security is based on global interconnectivity, where security responses are not considered as a pure national or state concern, in the same way as previous threats. Instead, the governance forms developed have a much broader application to cover the different fragmented cyber-areas. However, no one will be able to come up with a formula on how the virtual world can be securitized effectively until every possible security actor can agree about it globally.

I claim that the securitization is problematic in its application because it covers up the traditional legal processes and disturbs the balance of power. Moreover, there are problems with the extended use of securitization, as Roe has correctly argued. Roe states that securitized issues have the potential to disrupt the processes of open and accountable government. Through its very nature, fast tracking serves to limit the proper functioning of normal politics. The problem is that while the legislative process is

[454] Buzan et al. (1998),29.

[455] *To highlight the core element of securitization; the theory is just an analytical framework – it is not the theory's fault that a wide number of security issues are being securitizes rather than dealt with through normal politicized processes. This is the security actors, who overdue their role and make the process a norm rather than an exception.* Wæver (2011),468, 470.

[456] Tsoukala (2004) 'Democracy against security',435. Zedner (2009),124.

[457] Neal (2012a),260. Cf. Gross (2000) 'Exception and emergency powers', 1836. Fitzpatrick (2003) 'Speaking law to powers',251. Ramraj (2007) 'Between idealism and pragmatism',187.

[458] Neal (2012a),261.

surely accelerated, a degree of scrutiny and oversight nevertheless remains.[459] Even though the traditional methods of control and balancing are in place afterwards, the use of securitization is open to abuse, as practices and processes are developed in a secret area outside the normal democratic processes.[460] Therefore, the securitization processes should only be used as the last resort. The way in which the NSA and GCHQ have used securitization to justify meta-data collection is an example of how the power erodes over time, and it becomes standard to expand the legitimacy given in the speech-act.[461]

4.5 Rethinking Securitization in the Internet Age

I think that the rethinking of securitization is very interesting, although it appears fragmented and incomplete in order to comprehend the nature of cyber-space. Nissenbaum and Hansen review the original approach by applying it to cyber-security in an attempt to close a significant gap in the Copenhagen School’s framework by adding security dimensions that had not previously been considered relevant.[462] The new perspective on securitization encompasses cyber-security as the sixth sector.[463] Additionally, Nissenbaum and Hansen include three areas to the new cyber sector, in which security can be understood. These are hyper-securitization, everyday security practices, and technification.[464] Nevertheless, the linear three-step process is still the same: Securitization is related to the speech act, securitization and desecuritization

4.5.1 Hyper-securitization

Hyper-securitization is linked to a hypothetical interpretation of the threat discourse and the measures introduced to counter it. This differs from the original securitization approach because of its instantaneity and interlocking effect. This area is developed, not only from securitization of the network itself, but also from how much disruption a damaged computer system could cause social, political, financial and military breakdowns. As a result, other sectors and referent objects could have been damaged.[465] Hyper-securitization can be applied to an existential threat, where there is a possibility of damage and the identification of an immediate large-scale cascading disaster

[459] Roe (2012) ‘Is Securitization a 'Negative' Concept?’,260. Neal (2012a),261.

[460] Buzan et al. (1998),28.

[461] *It was revealed that the British Intelligence agency, the GCHQ, had secretly gained access to the network of cables that carry the world's phone calls and Internet traffic. Moreover, the agency was processing vast streams of sensitive personal information, which it shared with the NSA.* MacAskill et al (2013a) ‘GCHQ taps fibre-optic cables for secret access to world's communications’. Hopkins (2013) ‘UK gathering secret intelligence via covert NSA operation’.

[462] Silomon and Overill (2012) ‘Cybersecurity’s can of worms’,12.

[463] Buzan et al. (1998). Hansen and Nissenbaum (2009). Hart (2011) ‘Mobilizing the cyber space race’. Nissenbaum (2005) ‘Where computer security meets national Security’.

[464] Hansen and Nissenbaum (2009),1163-1168. Garcia and Palhares (2014) ‘Reflections on Virtual to Real’,276-277.

[465] Hansen and Nissenbaum (2009),1164.

scenario.[466] This form of securitization is useful when the cyber-attack is identified, immediate, and has moved from risk to threat. It is clear that this move calls for anticipatory governance forms, where the activities are necessary to pre-empt a situation that can have catastrophic effects. It is the level of uncertainty, which determine the method in use, i.e. risk-management or threat-assessment (chapters 2 and 3). However, I cannot see how hyper-securitization adds originality to the security framework because imagining and dealing with worst-case scenarios is already an integral part of risk-management and resilience/preparedness planning. The novelty is that securitization scholars accept that it is necessary to imagine scenarios on order to manage cyber threats.

4.5.2 Everyday Practices

The use of everyday practices is directed towards the way in which securitization actors mobilise ordinary individuals' experiences. The use of everyday practices has two directions. Firstly, to secure individual's partnership and compliance in protecting network security. Secondly, to make hyper-securitization scenarios more plausible as the use of individual's experiences links the disaster elements to everyday life. Nevertheless, I fail to see the pioneering significance of this approach because it does not deepen the security agenda by including an individual security platform to cyber-security. The new move is understood in a way where the acceptance of public security discourses may be compatible with the concrete experiences of the audience. However, this does not imply any real innovative management forms, which could improve governance.[467] This change illustrates a little step away from the pure state-centric approach originating from Copenhagen School, but nothing more than that. Silomo and Overill have correctly contested the use of individuals, arguing that individuals are merely considered as informants rather than being given an active position in the framework. As a result, Nissenbaum and Hansen circumvent important considerations regarding privacy, ethics, legislation and control, which would surface under a scrutiny of securitization of everyday practices.[468] Nevertheless, if individuals were given a more central role in the cyber-security process, the inclusion would significantly challenge the whole securitization approach. This would require an acceptance of the inadequacy of the securitization approach in dealing with new emerging risks of the Internet age.

[466] Garcia and Palhares (2014),276. Hansen and Nissenbaum (2009),1157.
[467] Hansen and Nissenbaum (2009),1165.
[468] Silomo and Overill (2012),17.

4.5.3 Technification

According to Nissenbaum and Hansen, technification gives room to technical experts to carry out the speech-act.[469] By giving technical experts this position, Nissenbaum and Hansen indirectly admit that the original securitization approach is too narrowly constructed because it only gives the securitization actors a voice in framing the security problem. The two scholars claim that the knowledge required to master cyber-space and the Internet is daunting and lacking in the public debate. Moreover, the pace at which new technologies and cyber-attack forms are developed adds to the legitimacy granted to computer and information experts. Technification gives experts privileged roles similar to the traditional security actors (chapter 2).[470] However, Silomo and Overill also correctly contest this. They argue that Nissenbaum and Hansen should be open to other forms of communication when considering the realm of cyber-space.[471]

Nissenbaum and Hansen exclude all other experts (none-technical experts/scientists), who may have knowledge about risk management or managing in vulnerable areas, because they do not consider them to be computer and information experts. Because the private sectors own and operate the majority of CI and CII, they have a high level of expertise in risk-management and resilience building. Despite their specific knowledge in various areas, these actors are not accredited experts in the technification context. From the security perspective promoted in this thesis, I believe that this creates a significant gap between theory and the substantive cyber-security management groups, because individuals are the first line of defence for their facilities. Therefore, they have particular and specialised knowledge that can be involved in developing guidelines and practices.[472] As a result, they invest in security as a necessity to assure consumer confidence. Moreover, these owners and operators have developed information about how to adjust their planning, assurance and investment programs to accommodate the increased risks of cyber-attacks.[473]

I believe that the rethinking of securitization from a cyber-security perspective still falls short of integrating the core problems of cyber-security in the analysis. Despite accepting the use of worst-case scenario imagination, and extending the scope of actors to include technical experts/individuals, Nissenbaum and Hansen are unsuccessful

[469] Garcia and Palhares (2014),277-278.
[470] Hansen and Nissenbaum (2009),1167.
[471] Silomo and Overill (2012),17.
[472] Garcia and Palhares (2014),277-278.
[473] Deibert (2002),129.

because they do not recognise the growing number of security actors necessary to manage the area. The two scholars recognise only security actors, who can carry out a successful speech-act. I think that this scope is constructed too narrowly because the threat level is much more fragmented and diverse and goes in both a transnational and a cross-sectoral direction by including groups and individuals. All computer users have the responsibility to protect systems and networks to increase cyber-security. This signifies that a large group of actors are involved in the management of cyber-space, and this cannot be watered down to just state actors and technical experts. These additional actors have a role to play in developing governance forms and practices, to engage people in the security management, and to raise awareness. However, the real dynamic in cyber-security lays in the networked formation, where there is a free exchange of knowledge between the actors to anticipate as many risks as possible (chapters 5 to 6).

4.6 The Paris School on Security

In this thesis, the Paris School can be seen in succession to nodal governance because they share a number of the same parameters for interpretation multileveled security. I would argue that what distinguishes the Paris School from the Copenhagen School's construction of the threat-nexus is its management of unease. The Paris School's security perspective is not a linear process like the Copenhagen School's perspective of securitization, nor is it clearly defined what signifies (in)securities/the management of unease. The Paris School is critical of Copenhagen's state-centric approach, and they claim that by focusing exclusively on discursive practices the Copenhagen School overlook some of the important non-discursive practices of security formations by agencies.[474] The Paris School's scholars provide a critical assessment of the liberties of citizens and others living in the EU Member States. Moreover, they analyse the way in which the EU population is affected by the proliferation of discourses about (in)securities, such as practices of reassurance, protection and coercion of governments and transnational agencies. All these are enacted to enhance safety of citizens or their collective security.[475]

The Paris Schools' security perspective concerns ordinary democratic policies and, therefore, it is placed in the realm of the politicised area of the security spectrum. Bigo

[474] Dunn Cavelty (2008),26.

[475] Bigo et al (2009) 'The challenging landscape of European liberty and security'.

claims that (in)securities/the management of unease does not result from one particular system of exceptionalism or an exceptional moment of emergency where normality is suspended - and in which rules are determined by the outstanding event.[476] Instead, the Paris School uses Foucault's perspective on governmentality by focusing on the way particular security issues are routinely managed by security actor. For example, the school critiques how bureaucrats or professional managers of unease undertake practices of surveillance and border control.[477] The primary focus is on the creation of networks of experts of (in)securities, the systems of rationalities they create and the productive power of their practices.[478] This area focuses on the widespread concerns about particularly illiberal practices used by contemporary liberal regimes.[479]

4.6.1 The Paris School and the Management of Unease

Bigo has stated that the growing number of (in)securities are based on the emergence of a continuum of threats, risks, and daily unease and this perspective can be interpreted from a Foucaultian perception.[480] To Foucault, security is linked to the liberal view of freedom:[481]

> "[T]his freedom, both ideology and technique of government, should in fact be understood within the mutations and transformations of technologies of power. More precisely and particularly, freedom is nothing else but the correlative of the deployment of apparatuses of security. An apparatus of security. . . cannot operate well except on condition that it is given freedom […] no longer the exemptions and privileges attached to a person, but the possibility of movement, change of place, and processes of circulation of both people and things.[482]

The way security and governance have developed over the last decade is prompted by a desire to govern beyond governing society. Instead, it is related to governing the responsibility choices of autonomous entities, which work independently from their organisation, i.e. governments, public and private sectors, enterprises, businesses, community groups and individuals. Within these rationalities, security was introduced in a way, which does not place the state central as the sole guarantor of security (section 3.3).[483]

[476] Bigo (2008c) 'Security. A field left fallow',105.
[477] C.A.S.E. Collective (2006),457. McDonald (2008b),570. Bigo (2002) 'Security and immigration',65. Cf. Huysmans (2006) *The politics of insecurity*.
[478] C.A.S.E. Collective (2006),458
[479] Bigo et al (2009),284.
[480] Bigo and Guittet (2011) 'Northern Ireland as metaphor',487. Joseph (2010),226. O'Malley (2009),2.
[481] Lentzos and Rose (2009),233.
[482] Foucault (2009),48-49. Lentzos and Rose (2009),233.
[483] Lentzos and Rose (2009),233.

The Paris School focuses on the interaction between security actors and their power distribution in closed security nodes. These involve practices, audiences, and safety procedures linked to handling security as a technique of government.[484] Bigo has extended the understanding of the securitization process from being an emergency process to constructing and applying security to several issues and areas in the politicised area.[485]As a result, the Paris School only includes a restricted part of governmentality, which contains three essential elements: the internal-external nexus, policing of (in)securities and interaction between security actors. I perceive the Paris School and nodal governance as different branches of the same Foucaultian tree, rather than entirely different perspectives. However, the focus of this thesis is broader than the Paris School because it includes a larger networked formation with numerous security actors beyond security professionals. Cyber-security concerns nodal governmentality in the networked structure, the interaction between framing cyber-risks (mentalities) and developing anticipatory responses (governance) on the strategic level and a variety of security actors, both governmental and non-governmental.

According to the Paris School, security procedures do not allow for exceptional measures, but security does not have a constitutive effect on the normal.[486] From this perspective, governments, and their bureaucracies have used this method to obtain control over the political processes at the expense of parliaments and oppositional political actors.[487] This transformation happens within the normal politicised area, contrary to securitization. The core element is when security actors take on their responsibility to impose security; they need to be subjected to appropriate normative scrutiny in a way that can justify the security measures imposed.[488] Using this logic, exceptional politics do not require new policies to deal with exceptional security problems. The security experts and the management of unease define security processes within society on a daily basis. Therefore, exceptional security practices derive from the ongoing processes of technocratic, bureaucratic, market-driven routines and normalisation.[489] I consider this to be considerably different from the Copenhagen School and their way of seeing exceptionalism. Yet, this is also open to abuse and policy creep as the procedures and governance forms become normalised, and the

[484] C.A.S.E. Collective (2006),457. Cf. O'Malley (2009),2.
[485] McDonald (2008b),570.
[486] C.A.S.E. Collective (2006),456.
[487] Buzan and Hansen (2009),217.
[488] Tadros (2007) 'Justice and terrorism',663.
[489] C.A.S.E. Collective (2006),466.

exceptional measures are introduced to bureaucratic routines. The work of the Paris academics has redefined normality as constituted by professionals through technologies of ordering and managing problems. The power struggle shifts from the political to the institutional level, where the security actors are involved in redefining the threats and the techniques to govern them.[490]

4.6.2 The Internal-External Nexus

In modern security, the internal and external dimension has become blurred. There is no longer fixed boundaries between them. To the Paris School, areas such as the police, customs, border guards, immigration officers, etc., are now positions central to security management. This is done due to their productive power, which seems to be suited for managing contemporary challenges because of the changes in the security perception.[491] Bigo et al. criticise the shifts in governance and the merger between internal and external security. They are paying particular attention to the consequences in terms of accountability and the position of individual citizens towards competent authorities. Their research has revealed that there is a problem in relation to the various shifts between competent levels of governments. One area of their research is related to the possibilities of political accountability, control and legitimacy through representative assemblies and their alternative forms. A second area of their research is linked to the position of individual citizens - and especially the consequences of their legal protection.[492]

The approach of the Paris School decentralises the state and thereby enhances the focus on several professional security actors, such as individual actors, institutions, and the networks of the security professionals involved in the process.[493] Correctly, Bigo has argued that the actual system of security officials does not respect the normative borders dividing inside/outside, national/international, and police/army. The structure is more fragmented and differentiated in its formation. The structure and processes of security professionals' breach the state-centric methodology and work in a complex and often entwined way regardless of agency, nationality or commercial entity.[494] I see this as the most significant problem regarding the use of nodal governance, as the whole systems is so fragmented, and nobody wants to take ultimate responsibility. Therefore, the actors

[490] C.A.S.E. Collective (2006),457. Wæver (2004),10.
[491] C.A.S.E. Collective (2006),459.
[492] Bigo et al (2009),296. Tekofsky (2006) 'Security in European external border law',19.
[493] Salter (2008a) 'Imaging numbers',247.
[494] Salter (2008a),247.

leave the problem to another authority, because whoever was in charge at the moment of inception is less likely to be blamed.[495]

Bigo and Guittet have argued that by making a separation between internal and external threats, or by focusing on what the global is, the discourses on (in)securitization arrange their arguments about these dangers. However, this form of discourses brings into question public liberties, the right to privacy and equal access to the law. These are all areas, which prevents the mounting of any legal resistance to coercive practices, even in a liberal state.[496] Bigo claims that Foucault refused to look at security as an exception; neither did he relate it to survival, war or external security.[497] This stance clearly separates it from the securitization theory. This has resulted in a particular perspective on security, where the focus of the Paris School is on the multiplicity of interaction between external and internal threats. It has been accepted that the fight against insecurity includes widespread coercive responses in order to end unpredictable violence or crime spreading from the local level to national, regional or international level.

The Paris School has proposed that the process should be an authorised form of practice of the bureaucracy, and not only the practice of the political power actors.[498] I think that this perspective is interpreted too narrowly. Cyber-security is based on a wider set of security actors. Beyond professional actors, there are public and private agencies, the routine actions of the consumer society and the condition of the possibilities of these claims and acceptance.[499] The Paris School simply leaves out the entire individual approach, where citizens and corporations are involved in cyber-security beyond formalised networks. However, they correctly argue that the networked security formation and internal interactions create problems with oversight and accountability. Bigo importantly stresses that some of the (in)securitization moves conducted by the bureaucracies or private security actors, are so embedded in these routines that they have never had been debated in a wider context as exceptional measures. On the contrary, the security moves are wrongfully seen as the continuation of routines and logic of freedom.[500] For example, surveillance is so pervasive and has so many

[495] Bigo et al (2009),291. Cf. Bigo (2006b) ‘Protection: Security, territory and population’.
[496] Bigo and Guittet (2011),491-492.
[497] Bigo (2006a) ‘Internal and external aspects of security’,389. Bigo (2008c) ‘Security. A field left fallow’,106
[498] Aradau and van Munster (2007),90.
[499] Bigo (2008b),128.
[500] Bigo (2008b),126.

dimensions, that it has become normalised to the extent that it is publicly acceptable to many.[501] However, what I find concerning is that different types of surveillance and monitoring techniques are introduced without being subjected to public scrutiny. Moreover, it is not clear when the information is used, and for what purpose. The uproar regarding Google street map and the infringement of privacy has turned into public acceptance, and no one has asked critical questions about this service.[502]

4.6.3 Policing (In)Securities

Policing insecurities does not signify that security is opposed to insecurity. Security can be collective and individual, and it is a consequence of broadening the security agenda by transferring policing methods into world politics, and contrarily the routinisation of military operations are visible in the national area.[503] Bigo and Guittet have argued:

> "[T]he core of the discourses on global terrorism, the transnationalization of the threat has become an argument that blurs the frontier between enemies and criminals, between the activities of the police in the criminal, intelligence and surveillance fields, on the one hand, and law enforcement's interventions targeted against an infiltrated enemy, on the other".[504]

This approach concerns the actual management (policing) of the Internet, on the one side, the formation of police networks and the politicisation of different security functions, i.e. surveillance and intelligence gathering as well as blocking and filtering content (sections 5.8.2, 6.8.2). According to Bigo, the processes, and practices developed in transnational networks constitute a threat. Security actors, which are involved in poling cyber-space, are structured in a differentiated way. Bigo et al claim that the integration of internal and external security discourses and practices destabilises the boundaries between the police, intelligence services, military forces and other special agencies involved in the management. This approach circumvents constitutional and democratic principles when security professionals develop rules internally in the nodes. Judges, lawyers and non-organisations are not being heard – and in order to prevent maximum security, which has potential worst-case scenarios inbuilt, it is necessary to strike a balance between security and liberty.[505]

[501] Bauman et al (2014),142.
[502] Bowers (2008) 'Our house, in the middle of Google's street'.
[503] C.A.S.E. Collective (2006),457-459.
[504] Bigo and Guittet (2011),491. Bigo (2008a) 'Globalized (in)security',10. Cf. Bigo (2000) 'Liaison officers in Europe ',67. Kaunert (2011) 'European internal security-towards supranational governance in the area of freedom, security and justice?' Schroeder (2013) *The organization of European security governance.*
[505] Bigo et al (2009),302.

By transferring decision-making to security, professionals create a one-sided perception of the problem.[506] However, I find policing cyber-space in an external and internal context very problematic. Kremer highlights that it is important to look at what drives the protection of individuals from harm and he searches for a balance between individual freedom, rights and individual as well as collective security interests. In cases of interferences with rights in cyber-space, the security measures require that justified and adequate safeguards are included. Criminalisation, can hence provide a tool for countering security problems in cyber-space, but at the same time provide certain procedural safeguards.[507] Yet, it is more difficult when it comes to implementing these types of strategies globally or regionally (sections 5.4, 6.5). This leaves the space open for developing rules and regulations to manage the area until legislation is adopted and harmonised across the security spectrum.[508]

I side with Kremer, when he claims that the threat of cyber-crime needs to be critically assessed. Criminalisation can become a political tool and an avenue for security mission creep, which can transfer specific interests into criminal law. Moreover, the lack of regulation can open up justifications for more control and surveillance. From the mind-set of the Paris School, it is important to strive for a balance between security and liberty. However, the way security professionals frame cyber-risks can change the balance of the focus on worst-case scenarios.[509] According to the Paris academics, governments, security companies and the media cynically play on the fear factor in order to introduce more security measures. It is not only governmental security actors, who use the worst-case scenario technique to maintain security. Fear also plays a significant role in different areas. For example, corporations cynically trying to sell their new security equipment and skills, and the mass media's overarching goal of selling news, where security is always a good area for creating 'good guys vs. bad guys' news reports.[510]

This differentiated approach to security blurs the field and creates a fragmented form of governance.[511] These specialised groups are mixed up with international actors, where the profession, the organisational level, the mission, the data and the technological

[506] Bigo et al (2009),302.
[507] Kremer (2014) 'Policing cybercrime or militarizing cybersecurity?',234
[508] Kremer (2014),234.
[509] Kremer (2014),235.
[510] Bauman et al (2014),142
[511] Bigo (2008a),20.

innovations flow between the actors on many levels.[512] Bigo perceives this as a threat. He warns against the enhanced use of security agencies, stating that this development undermines security by competitively merging the questions of policing and defence.[513] I slightly disagree with Bigo’s assumption. I regard the use of different security networks as a necessity to manage transboundary risks, threats and dangers. Particularly in relation to cyber-security, a broad formation of security actors with specialised knowledge is required.

4.6.4 Networked Structures

Networked structures have obtained a firm hold in security strategies based on their status, roles, activities and institutional settings.[514] According to Neal, these structures are based on technology, knowledge and methods of governing rather than simply ruling.[515] Governmentality is essential to framing and responding to security issues. Particularly in relation to cyber-security, where technology and knowledge are central and developments require constant reviews of rules, practices and processes (section 3.3). Foucault emphasises that there is not only one system involved, but also a multiplicity of formations of actors and systems.[516] The structure of these networked systems has to be loosely created as well as changeable in order to retain the flexibility. There is also a need for cooperation among the security actors. Security actors promote a mixture of information, experience and scientific techniques, which could be utilised in order to develop a sustainable security structure whether it concerns state or non-state security issues.

In order to deal with cyber-attacks, such as the Heartbleed bug, multileveled cooperation is needed to manage the problem. I believe that the interconnectivity is the biggest problem with cyber-security management because globalisation has made it impossible for one single actor to impose security, i.e. risks, threats and dangers. As a result, I consider that there is an increased need for establishing networks between security actors to exchange information and develop pre-emptive and preventive measures to control these transnational and cross-sectoral threats. However, the Paris School has critically analysed the practices and technologies used in these networks, and argued that due to their diverse foundation they are open to abuse of power. This

[512] Bigo (2008a),20-21.
[513] Huysmans (2006) ‘Agency and the Politics of Protection’,13.
[514] C.A.S.E. Collective (2006),458.
[515] Neal (2008),47.
[516] Foucault (1994a),205–206.

approach can be transferred to the metadata collection methods developed by the NSA and GCHQ, and this distribution of power is a clear example of abuse and exceptional measures developed internally in the security agencies.[517] For example, the phone tapping carried out by security actors went so far that it included the German Chancellor Angela Merkel.[518]

Security cooperation contains two elements. Firstly, different actors work together in nodes, which link state and non-state actors together in loosely defined networks. Secondly, each security node works both independently and in cooperation on a case-by-case basis, where the security issue determines who participates. The Paris School claims that it is possible to identify changes from the Snowden revelations in 2013. It is visible that security is organised, neither within the state acting within a transnational context, nor an emergent hierarchy of the kind envisaged by globalisation theorists. Moreover, it is not possible to transfer the idea of a new empire or concert of great powers to the system. Instead, it is suggested that something less predictable is occurring, and this unpredictability is linked to security agencies, such as the NSA or GCHQ, which practices challenge the assumption of democracy by developing intrusive security measures from their interactions.[519]

I consider the routinised conduct of security to be dangerous as security actors over time extend their mandate for the security measures. This is open to an abuse of power similar to securitization, although it is carried out in the politicised area. The Paris academics are critical of security governance and practices developed in the different nodes positioned outside public scrutiny. Unfortunately, this governance form leads to mission creep in areas where accountability and transparency are missing (sections 5.7, 6.7, 7.4.4). Yet, this is a part of the nodal security dynamic, where the hieratical structure is down scaled. The mission creep is visible in measures introduced by the UK Government in relation to the proposed Counter-terrorism and Security Bill (2013).[520] This bill includes a requirement for internet service providers to retain data on internet protocol addresses to allow individual users to be identified. In this context, there is a blur between intern and external security as well as policing. The new law requires Internet and phone companies to generate the records, retain them, and hand them over

[517] Ball et al (2013). Cf. Bigo et al (2013) ‘Open season or data fishing on the web’.
[518] Oltermann (2014) ‘Merkel urged to press Obama on NSA scandal ahead of Washington talks’
[519] Bauman et al (2014),135.
[520] Government Bill (*2014)* ‘Counter-Terrorism and Security Bill 2014-15’.

to the police and security services on request.[521] Moreover, the bill proposes measure to manage online child-abuse in the dark net TOR.[522] This also signifies a development, which has the potential for abuse in terms of creating more insecurity online.[523] Looking for abuse of children on the dark web is just a way of searching for, and identifying the source and recipients of a prohibited class of information. However, the net does not differentiate between information. Here it is all the same, so by allowing these agencies to develop legal mechanisms to identify one sort of prohibited information, they are opening a Pandora's Box for a similar mission creep where similar types of information flow can appear in other areas. This gives access to introduce governance forms and practices to identify any prohibited information beyond the original justification.[524] These policies are firstly introduced in a security area (child abuse), where most people will accept harsh measures. However, the problem arises concerning the trade-off when people recognise that the same actions are targeting citizens beyond these original justifications, and suddenly ordinary areas are becoming part of the same intrusive form of surveillance. Moreover, I find it concerning that the GCHQ will be given a central role in this bill; this is the same agency, which has been widely criticised for its intrusive methods and mission creep in the Snowdon revelations (sections 5.8.2, 6.8.2).[525]

4.7 Comparing the Two Security Schools and their Influence on Anticipatory Governance and Practices

The discussion has so far demonstrated that the way security is framed is clearly a rather contested issue, and it is possible to speculate on how different strategic responses would emanate depending on the conceptual framework adopted by a particular government/organisation. I argue that the high level of uncertainty in risk makes it incompatible with management processes by threat-assessment strategies because they do not accommodate the significant structures of risk (chapters 2 and 3). By having risk included in their perspective, the Paris School encompasses anticipatory governance and that positions them closer to cyber-security strategies compared to the Copenhagen School. The development of cyber-security strategies means that the threat-security tandem is longer seen as the primary approach. Threat-based policies are still relevant to

[521] Travis (2014) 'Counter-terrorism and security bills'.
[522] "*Tor is a popular 'darknet', a network that aims to conceal its users' identities and online activities*". Spitters et al (2014) 'Towards a comprehensive insight into the thematic organization of the Tor hidden services'. Watt (2014) 'Dark web'. Cf. Maras (2014) 'Inside Darknet: the takedown of Silk Road'.
[523] Watt (2014).
[524] Watt (2014).
[525] Ball et al (2013).

the cyber-security structure. However, I have chosen to position it peripherally as a last resort strategy in place when the preventive measures fail to deal with the risks (section 3.7). Because of the different foundation in security, two areas are incorporated in cyber-security. Firstly, anticipatory strategies are located before threats in order to create a margin of safety.[526] Secondly, security in the world risk society is extended to involving new security processes. This includes interactions between actors, organisations, levels, regulations, practices and processes that embed transnational and cross-sectoral cooperation (sections 5.6 and 6.6). In this area, the Paris School is influential, using governmentality to manage the large number of security actors and measures developed in a differentiated and fragmented context beyond the direct exercise of the state.[527]

On the other hand, I think that Paris School's analytical framework fails to consummate all the issues in the cyber-security management. They have a narrow scope in relation to generating insight into the development of anticipatory governance and practices beyond the role of the security professional. In this thesis, I claim that the cyber-security cannot be reduced to routine practices of anticipatory governance and interactions of security professionals. Cyber-security involves a broader mixture of security actors. This can be state actors working alone in their formation; they can interact with the private sector, experts, groups or individuals. These actors can also work alone in different networks, without any state involvement. Finally, individuals can execute a personalised security regime independently. The Paris School analyses how security professionals use their bureaucratic authority to categorise and assess the threats and determine what constitutes security. However, the management of cyber-security goes beyond this, as it also concerns individual security. This means that security management does not necessarily have a professional element, and the governance forms, and practices useful for cyber-security are found in the space between these two schools.

The European cyber-security framework is not a part of the 'exceptionalistic' security process. Instead, it is founded on a preventive form of logic (section 3.6). The strategic goal is to intervene before the situation spins out of control and calls for exceptional

[526] Sunstein (2005) 'Laws of fear',13.

[527] Bigo and Tsoukala (2008) 'Understanding (in)security',4. Joseph (2010),225.

measures.[528]As a result, I believe that European cyber-security management forms are better suited to exploring varieties of fragmented security issues by incorporating nodal governance in the framework (sections 3.3, 5.3). Security actors are shifting the focus from defence to technologies and strategies in which the future is made calculable and manageable as part of the politicised area, rather than exceptional measures.[529] This approach can be compared with the perspective incorporated in the Paris School as cyber-security processes go beyond the narrow application of securitization. Therefore, the change can be illustrated by the evolution of security from a direct exercise of state power (the Copenhagen School) to an inclusive method of power, which is exercised through the security networks of institutions, practices, procedures and techniques to regulate social conduct (the Paris School).[530] Consequently, risk-management draws on the legitimacy from the politicised area similar to the Paris School. This signifies that governance structures and practices use politics based on best estimations and most likely future scenarios. These are considered as the best guidance for assessing dangers linked to cyber-space and the use of computer technologies[531]

European strategies focus on the most suitable security solutions playing on ‘safety first’ management methods in order to enhance resilience.[532] The way cyber-security is framed is mostly in line with the academics behind the Paris School’s perspective rather than the Copenhagen School’s securitization approach. It is simply not possible to discuss risk in the light of exceptionalism and the survival of a given referent object. If so, many risks would fall under the scope of securitization, and it is simply not possible to manage them all as exceptions; it would destroy the meaning of exceptionalism. However, it does not signify that that idea behind the Copenhagen School’s securitization is outdated. It can be useful to closed networks, such as a local area, a national state or internally in cooperation or group, where the threat of an attack becomes evident, and a fast response is needed. However, to impose restrictions, such as the ones in the Twitter case, have no particular effect and is a waste of resources and capabilities, because the securitization process has shown its limitations in cyber-security. The main argument, for linking cyber-security to the Paris School, is that the

[528] Van Munster (2005) ‘Logics of security’,8.
[529] C.A.S.E. Collective (2006),469.
[530] Joseph (2010),225.
[531] Corry (2010),18.
[532] Corry (2010), 18.

securitization approach is unable to grasp the every-day formation and development of new security issues in the ordinary sphere.

The rethinking of securitization is very interesting and relevant, and I have included it in the analysis on behalf of the original security approach. It shows the willingness of the academics involved with the Copenhagen school to forward their security approach into a new generation of security studies (Nissenbaum and Hansen). However, I see this as a work-in-progress as it appears fragmented and to some extent, disconnected to the real issues of cyber-security. The Copenhagen School take into account the central features of cyber-security and make the necessary opening for introducing the sixth sector, hyper-securitization, every-day practices and the use of technical experts. Yet, the traditional interpretation of security cannot be directly transferred to cyber-security as there is not one referent object, but numerous, as well as a large group of securitizing agents. Interesting enough, their rethinking of securitization includes new actors beyond the state. However, Nissenbaum and Hansen abstain from addressing the crucial issue of multi-agency cooperation on the horizontal and vertical level central to anticipatory cyber-security governance. To my disappointment, the new perspective falls short of identifying the depth and the breath of cyber-security and the user's responsibility to protect the network. Thereby, they still keep an elitist approach to security, where individuals are only given a partial role to pass on information. As a result, they fail to recognise group′s and individual′s responsibility as first-line security actors. Nevertheless, I find the updated version of securitization useful as a supplement to the Paris School′s interpretation of governmentality (section 3.3). There are difficulties in describing and analysing complex empirical realities, which challenge the security discussion and the use of the two schools. Nevertheless, I use their analytical lenses to generate significant insight into cyber-security governance and practices.

4.8 Synthesising a Theoretical Framework

Following the discussions in chapters 2, 3, and 4, I syntheses the theoretical framework to progress the discussion and bridge the theoretical foundation for understanding cyber-security with the substantive analysis. The main areas for progressing the debate are nodal governance and anticipatory risk, as they are the underpinning concepts. The existing literature discussed in the theoretical framework has showed gaps in addressing European cyber-security governance forms that include both transnational cooperation and cross-sectoral cooperation.[533] In this second part of this thesis, I focus on qualitative documentary analysis based on the research objectives presented in the first chapter.

In the two case studies, I focus on the development of cyber-security governance in two distinct areas. Chapter 5 covers the general and the overarching concept of cyber-security, and chapter 6 examines the sub-category of cyber-terrorism. The scope and limits of this empirical work relate to the challenges of cyber-security in Europe. The EU develops the primary security strategies, and these are used to outline the broad perspective based on risk and cooperation. The CoE and NATO draw up supporting cyber-security policies and initiatives, which are used to advance the arguments. I have designed the figure below to illustrate the three-step process included in cyber-security that forms the foundation for the substantive analysis. The involvement of multiple security actors is central to the analytical framework because cyber-security governance is based on cooperation among a large group of powerful actors, i.e. state authorities, industry associations and large enterprises to provide the necessary security and expert power.[534] As a result, this study emphasises cooperation and anticipatory governance forms. By having this focus, governmentality becomes highly relevant, as it is the awareness of the plurality of the different units that shapes modern forms of power.[535] In view of that, I use both the Copenhagen and the Paris Schools′ security approaches to analysing existing cyber-security strategies (figure 2).

[533] EU (2003). EC (2010j) 'The Stockholm programme'. EC (2010e) Delivering an area of freedom, security and justice for Europe's citizens'. EC (2007b) 'Towards a general policy on the fight against cyber crime'. EC (2009b) 'Protecting Europa from large scale cyber-attacks and disruption'. EC (2011a) 'Achievements and the next Steps', EC/HRECFASP (2013) 'Cybersecurity Strategy of the European Union' .CoE (2001) *Convention on Cybercrime*. Podgor (2004) 'Cybercrime: National, transnational or international?. NATO (2013) 'Partnership', Kendall (2004) 'Global, international and actor network'. Kock and Buser (2006) 'Emerging metagovernance as an institutional framework for public private partnership networks in Denmark'. ENISA (2014b), Provan and Kenis (2007) 'Modes of network governance'. Woods and Sharing (2007), Coker (2002) *Globalisation and Insecurity in the Twenty-first Century*. Yeung (1994) 'Capital, state and space', Beck (2009).

[534] Schmidt (2014),181.

[535] Ransom (1997) *Foucault's discipline: The politics of subjectivity.*16. Barnard-Wills and Ashenden (2012),114.

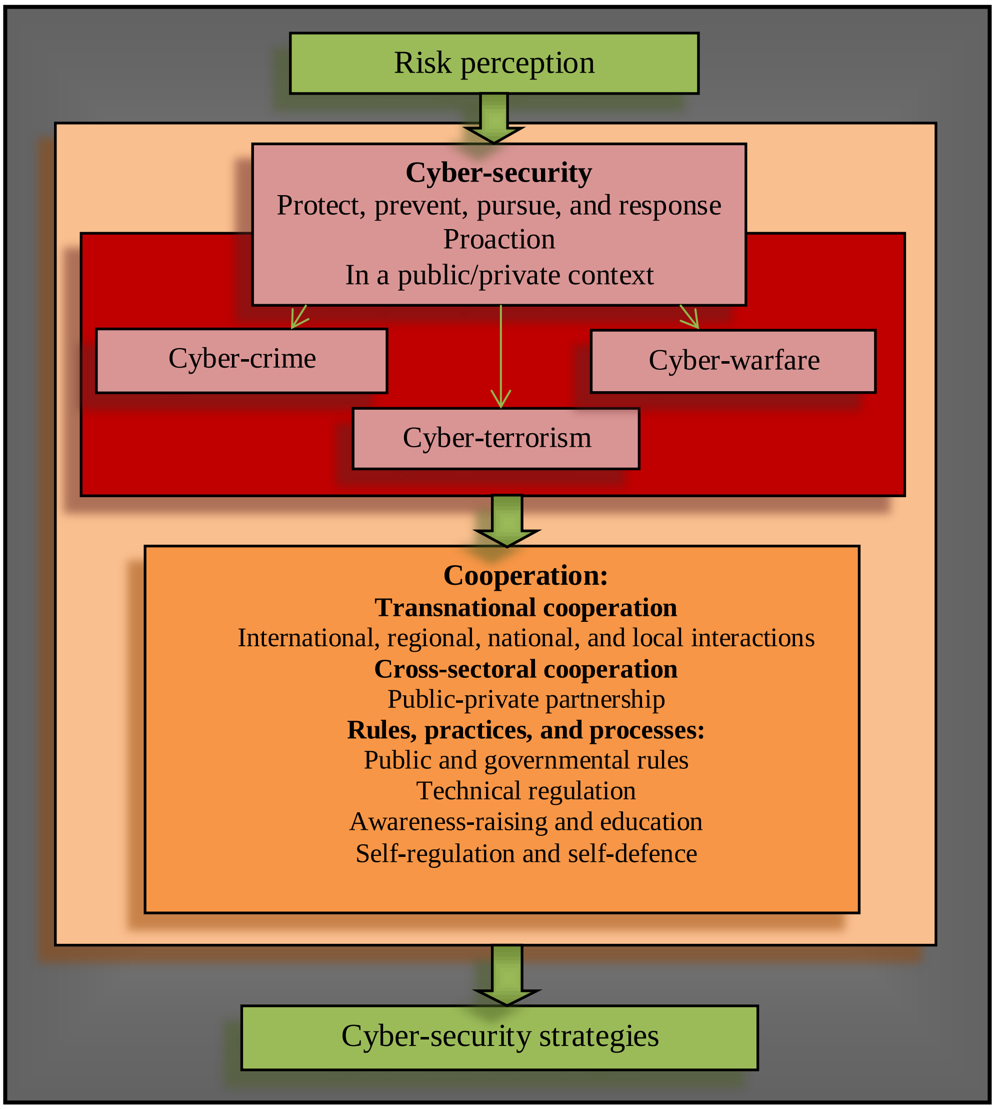

Risk perception
Cyber-security
Protect, prevent, pursue, and response
Proaction
In a public/private context
Cyber-crime
Cyber-warfare
Cyber-terrorism
Cooperation:
Transnational cooperation
International, regional, national, and local interactions
Cross-sectoral cooperation
Public-private partnership
Rules, practices, and processes:
Public and governmental rules
Technical regulation
Awareness-raising and education
Self-regulation and self-defence
Cyber-security strategies

Figure 7 model for advancing the analytical framework

The areas, I have included in the substantive analyses, are security actors, cooperation, and anticipatory governance, and these areas prevail in the most significant parts of European security strategies. The following discussion outlines this framework and sets out the methodology for addressing the research objectives in relation to cyber-security and cyber-terrorism. I claim that the cyber-security takes its outset from a hybrid-networked foundation, where security actors have an overlapping role, because they are underpinning features at all levels of the analysis (section 3.3). These different types of actors are linked together ad hoc in a networked formation of security nodes. Therefore, considerable resources and expertise for planning and taking protective measures lie outside governments and their institutions.[536] As a part of nodal governmentality, the power is distributed outside a singular forum from the strategic level down to the operational level. Accordingly, there are a broad number of governance forms developed to manage cyber-space, which spans from spectrum allocations, copyright and intellectual property regulation, content filtering and blocking and different types of cyber-crimes.[537]

4.8.1 Transnational and Cross-sectoral Cooperation

Cooperation between security actors has developed over the years, and I believe that this approach takes a central position in the cyber-security framework. In this part of the thesis, I have outlined how international institutions have been redefined and restructured in past decades. Moreover, the historical outline has shown how a number of state institutions and security actors (public and private) have mitigated the strict state-centric approach.[538] As a result, this thesis narrows down the state-centric approach significantly. Instead, numerous security actors have important roles to play based on their expertise and their incitement to be involved in the cooperation, and they can generate positive developments by bringing in different insight to problems and solutions. In this thesis, cooperation, the distribution of knowledge and the decision-making process are central. Therefore, I claim that the success rate of nodal governance is entirely in the hands of the security actors and their ability to pool together specific interactions, mentalities, technologies, institutional arrangements and resources.[539] Together they are able to enhance resilience in society. If security nodes do not succeed, they need to change its structure and re-organise the node in an ongoing process (section 3.7). Thus, the nodes are continually progressing, and this puts pressure on the security framework, and the challenge to security management is linked to the ability to cooperate, and develop, and harmonise rules, practices and processes.

Transnational cooperation is one of the cooperation types which influence governance structure in cyber-security because of the global aspect, where criminal activities can originate from the other side of the world.[540] It is a problem, that there is no universal consensus on the governance forms developed, and it has proven difficult to overcome

[536] Dunn Cavelty (2008),136.

[537] Deibert and Rohozinski (2010b),16.

[538] Haftendorn et al (1999*) Imperfect unions'.* Webber et al (2004) 'The governance of European security'. Gray (2007), 268. He (1995),77. Anderson (1996),239. Hough (2008),35. Weiss and Kalbacher (2008),327. Sheehan (2010),176. Craig and de Búrca (2008),3-4. Foster (2006),7.

[539] Shearing (2006) 'Reflection on the refusal to acknowledge private governments',26.

[540] Grabosky and Smith (2003b) 'Crime in the digital age',41.

the differences in legal systems, values and priorities worldwide.[541] The key element of cyber-security is to improve security of essential CI, CII and ICTs by enhancing and supporting a high-level of preparedness, security and resilience capacities on all levels (section 3.7).[542] The cross-border dimension of cyber-space related problems and the possibility to attack computer systems worldwide constitutes a growing challenge.[543] So far, obstacles for ensuring efficient management derive from judiciary limits, insufficient intelligence gathering/sharing capabilities, technical difficulties, disparate investigative and forensic capacities, lack of trained staff, and inconsistent cooperation with other stakeholders involved in cyber-security.[544] I would argue that the nature of cyber-security creates obstacles to governance forms, and it is impossible to only establish cooperation using traditional security processes to manage risks emerging multiple-directionally in the public and private sphere. In practice, alternative measures and procedures imposed to counter cyber-related crimes and attacks have opened new arrays of multi cross-sectoral governance.

In cyber-security, I have noticed that another form of the governance is developing within the cross-sectoral sphere. In this thesis, I have given public and private partnerships (PPPs) an essential role, because this governance form is growing to improve security. I believe that partnerships have a value in the framework because they establish new means of cooperation where the actors can develop newly innovative methods to assess the security risks. It alters the traditional government-business relationship by creating an equal partnership, where the new culture of cooperation replaces command-and-control governance. However, I find that this trend of multi-levelled cooperation driven by distinctive communities makes it even more difficult to improve transparency and openness, or outline an understandable governance structure, when the parties are changing all the time. I also find it problematic that the complex structure makes it nearly impossible to pinpoint accountability processes, unless an oversight mechanism is included in the security strategy (sections 5.7, 6.7).

4.8.2 Security Actors and Cooperation

In this thesis, security actors are central to developing anticipatory governance and practices, as these are developed outside the traditional management structure due to the

[541] Grabosky and Smith (2003b),41.

[542] EC (2011a),1. EC (2009a) ‘Commission acts to protect Europe from Cyber-attacks and disruptions’. EC (2009b),2.

[543] EC (2009b), EC (2009c), EC (2011a), EC/HREUFASP (2013).

[544] EC (2012b),3.

nature of the risks. The actors involved in cyber-security can come from both cooperation types, divided into different levels, in both transnational and cross-sectored formations. Within such pluralist approaches, governance originates from those associated with traditional electoral politics through inter-governmental activities to complete self-governance regimes.

Cross-sectoral cooperation has obtained a central place, and it is based on a particular relationship between the state and private industry. This implies that governance is based on the mobilisation of knowledge, capacity and resources of a variety of organisations, groupings and individuals. This encourages a number of security actors to participate and take responsibility for security within their interest domain (sections 5.6, 6.6).[545] The proposition is that the state governs better at a distance. Therefore, it is left to the individual actors to reach the level of security outlined by the public sector, and this can vary from voluntary self-regulation to mandated full self-regulation.[546] Accordingly, the state can set out priorities, such as minimum requirements, standards or objectives, where security actors respond and cooperate to fulfil these goals. This is done through market-like mechanisms orchestrated by state governments in order to ensure that state-defined objectives are achieved.[547] However, cooperation can also be developed outside the state coordinated by private security actors.

I argue that bringing in a variety of actors from the two sectors creates a challenge, as they have different reason to participate. Even in an equal partnership, there can be tensions between the security parties involved (sections 5.6, 6.6). Apparently, tensions derive from their roles in society, their organisation and/or their motivation to cooperate. Problems can arise from expanding the security field, extending the number of institutional actors and involving actors with contradictory interests who seek to maintain/enhance their positions.[548] In practice, these problems are not wholly distinct, and the tensions might not cause problems as their common goal interlinks the parties in a power-balanced partnership.

[545] Wood and Shearing (2007),12-14. Shearing (2006),24. Black (2002) ‘Critical reflections on regulation’,5. Loader and Walker (2007) ‘Civilizing security’,124-125.

[546] Scott (2009),52. Shearing (2006),24. Bartle and Vass (2007) ‘Self-regulation within the regulatory state’,889.

[547] Wood and Shearing (2007),11,18.

[548] Dupont (2006),87. Wall (2007),179. Schaeffer and Loveridge (2002) ‘Towards an understanding of types of public-private cooperation’,173.

4.8.3 Anticipatory Governance

The third area, which I explore in the substantive analysis, is linked to the result of cooperation. Cyber-security involves developing rules, practices, and processes relevant to security areas by involving a mixture of states, corporations, and civil-society actors, i.e. transnational and cross-sectoral (section 3.7).[549] In order to develop anticipatory governance forms and practices, I argue that it is necessary to go beyond the traditional legislative process. Nonetheless, legislation is still required, but it does not stand out as the most significant mean; it is merely a tool among others. The enactment of substantive and procedural laws is necessary to develop and manage anticipated cyber-risks.[550] However, I think that the most significant problem regarding legislation is the requirement for reaching a certain level of harmonisation because hackers do not respect physical and sovereign borders. As a result, tackling hackers puts pressure on sovereignty, and the issue of jurisdiction often creates problems.[551]

The expansion of cyber-space related crimes has generated a range of legislative and judicial responses, with a number attempting to encompass existing security measures with the new dangers from cyber-space. Particular challenges are presented by the inherently global nature of Internet interactions. As a result, an increasing number of international agreements complement the legal innovations at the national level. This is supported by informal regimes of governance and regulations implemented by non-governmental security actors.[552] It is clear that security processes are not imposed to develop exceptional measures. The work of agencies is subjected to the principle of accountability, whereby the actions can be challenged in the judiciary system, or through other independent and impartial mechanisms.[553] The security actors are, therefore, limited in their actions and can only participate in the cooperation as long as it complies with their rules, the legal basis and their different responsibilities. Public authorities are held accountable through the traditional institutionalised check-and-balancing system, whereas self-regulation of the conduct of non-governmental organisations is self-specified, self-enforced and self-monitored. Together these rules, practices and processes create governance forms, which emerge from transnational and cross-sectored cooperation (sections 5.8, 6.8).

[549] Coker (2002),29.
[550] Bullwinkle (2005) ‘International cooperation in combating cybercrime in Asia’,269-302.
[551] Grabosky (2007b),201.
[552] Yar (2006),39.
[553] Aquilina (2010),140.

Effective management in areas of high complexity, such as cyber-security, has a clear transnational approach due to the nature of the risks. The management of security risks is linked to developed norms among the regulated, which encourage them to comply voluntarily with the outcomes of the nodes, e.g. guidelines, practices, processes. The level of self-regulation depends on the creation of a constant and constructive dialog between the regulators and the regulated (responsive regulation).[554] From my own security perspective, regulation on a macro-level cannot be reduced to being just one instrument of the public sector. It provides a comprehensive framework, where business enterprises, citizens and governmental officials are active in the regulatory framework to develop regulatory responses appropriate to a particular security risk.[555] I believe that the private sector has a significant role to play in developing governance structures within particularly distinct areas where the government or regulatory authorities have no power. This creates a wider governance approach to progressing specific anticipatory security strategies.

4.8.4 Anticipatory Governance and Regulatory Practices

One of the biggest challenges, in securing cyber-space, is based on the interconnectivity. The Internet has developed as an open, decentralised framework, expanded globally beyond legislative and territorial boundaries, which is often considered its greatest strength in cyber-space (section 1.1). However, at the same time it is also an increasing weakness of the system.[556] I argue that because of the rapid technological advancements, it is impossible for regulatory practices and methods to keep up with technological advancement unless the regulatory forms and processes are expanded to mirror the changes in cyber-technologies. The problem is that the regulation cannot address in details all specific areas of computer technology and the associated risks. In cyber-security, no matter how much legislators and decision-makers try, they can never catch up with the fast progressing technology. There is always a danger that the legislative process is too slow and inadequate, and regulations end up addressing problems that are already passé.[557] I argue that several elements of current security strategies need to be reconsidered. In order to do so, it is important to get an insight into the way security is conducted, the parameters for cyber-security, and how the European region responds to the growing risks.

[554] Ayres and Braithwaite (1992) ‘Responsive regulation’,4. Moran (2002) ‘Understanding the regulatory state’,398.
[555] Hildebrandt (2008) ‘A vision of ambient law’,178.
[556] Yar (2007),55.
[557] Aquilina (2010),140.

I think it is important to analyses the regulatory framework and the measures used to enhance cyber-security. Firstly, it is important to look into harmonisation of state legislation, as there is an urgent requirement for harmonising cyber laws or at least making them compatible with other states′ legislative framework.[558] States have different priorities; some do recognise that particular forms of regulation are needed, and others do not recognise cyber-offences and regard them as falling under the scope of existing regulations. Given the technological, legal and cultural diversity of the world′s nations, the risk perception differs significantly (section 3.6). Some state priorities theft of intellectual property. Other states consider blasphemous or seditious communications to be their paramount concern. Finally, some states have the application of technology used to sexually exploit children at the top of their security agenda.[559] Technical regulation is another important area, which is developing in order to create obstacles to the free flow of information online. The technologies used to support cyber-security present an interesting paradox on the global and national level.[560] On one side, the measures to achieve greater cooperation at the international level for the protection of CI, CII and ICTs underlie the preservation of a free and open internet. On the contrary, there is an increasing divergence in the national efforts, as governments tend to impose restrictions. These measures impose limitations to the potential of global connectivity by filtering, blocking, surveillance of content, etc. The use of restrictions to the free flow of information violates the whole idea of free Internet (section 1.1). Moreover, it jeopardises the privacy of the users.[561]

I would argue that information sharing also constitutes a problem to the development of adequate responses to cyber-risks. This relates to the ways in which CI, CII and ICTs policies are conceived and implemented. In this context, I claim that the problem is that over the years measures imposed have been based on quick solutions, which were shortsighted and wrong-headed. As a result, many of the institutions failed to prevent the risk by using inadequate resources, which were poorly designed to respond to the dangers, and without the appropriate mechanisms to share information across borders.[562] An interesting feature in most cyber-security programs developed recently is

[558] CoE (2007) ‘How to prevent cybercrime against state institutions in member and observer states?. Uda (2009),41.
[559] Grabosky (2007b),207.
[560] Deibert and Rohozinski (2010b),15–32. Radu (2014) ‘Power technology and powerful technologies’,14. Cf. Murray and Scott (2002) ‘Controlling the new media’,500-501. Lessing (1998) *Code and other laws of cyberspace*,235-239. Lessing (1999) ‘The law of the horse’,508.
[561] Deibert and Rohozinski (2010b),15–32. Radu (2014),14.
[562] Deibert and Rohozinski (2010b),21.

the focus on cooperation, sharing knowledge and pooling resources and capabilities. As a result, there is a growing acknowledgment of community of practices across states and private actors to share a common vision of what is to be secured and why.[563] I link this to nodal governance, where the practices are developed internally in the security nodes to accommodate the absence of appropriate cyber legislation.

These forms of management can be developed by identifying the appropriate minimum standard and guidelines by using core principle to regulate the relationship between public security and the rights of the individual users, i.e. the right to privacy, data protection. The idea is to apply these core principles across the broad range of security measures and technological advancements. From that point, competent authorities incorporate these principles and guidelines with immediate effect to emerging technologies in a coherent, consistent and uniform way. This area is progressed rather than to await slow legislative processes. Nevertheless, this form of governance is a step back for developing appropriate cyber-security measures and legislation.[564]

4.9 Methodology

The methodology I have used in the following two chapters is based on documentary analysis, which enables me to investigate cyber-security governance critically within a confined area (section 1.4). The empirical research is based on two case studies related to cyber-security and cyber-terrorism. The insight gained from examining this area allows me to analyse the data collected concerning the parameters inbuilt in European cyber-security strategies. Moreover, this section has allowed me to engage with the tradition of grounded theory advanced by Strauss and Corbin and their way of identifying, colleting, analysing and concluding on a large group of data.[565]

In this section, I have outlined the research strategy used to define, collect and analyse anticipatory cyber-governance and practices, which are compatible with the theoretical part. I begin the analysis by identifying the research area by using the objectives outlined in chapter one. Moreover, I have collected data from different sources, which fall into four data groups. Firstly, I will examine European cyber-security policies, such as legislation, directives and communications from European institutions. Secondly, I

[563] Deibert and Rohozinski (2010b),21. Cf. Hansen (2013) *Security as practice.*
[564] Aquilina (2010),142.
[565] Cf. Strauss and Corbin (1990) *Basics of qualitative research: Grounded theory procedures and techniques.* Corbin and Strauss (1990) 'Grounded theory research: Procedures, canons, and evaluative criteria'. Corbin and Strauss (2014) *Basics of qualitative research: Techniques and procedures for developing grounded theory.*

have collected data from other academic studies and publications, which includes books, book chapters, reports, commentaries and journal articles. Thirdly, I have researched online, using states′, European institutions′, businesses′ and organisations′ databases, web pages, and archives. Fourthly, I have use press releases and news coverage by security actors and mass media, which have kept me updated with the latest development. Cyber-security encompasses a variety of security actors from public and private sectors, to organisations and individuals, which all have significant data published online. Therefore, it is necessary to include different governance and management forms.[566] However, in relation to cyber-security, I have used an extensive number of non-academic sources. I have been critical when examining the documented evidence provided by the research methods used in group three and four. Therefore, I have taken extra time to trace all the sources of these documents and searched for supporting evidence in order to validate the data.

4.9.1 Identifying the Area

Cyber-security is continually developing; therefore, documentary materials might be incomplete or missing. Over the last decade, the EU has created a cyber-security framework based on legislation and governance forms including directives, communications, programs, action plans and roadmaps, which will be included in the analysis. The rapid development of this area dictates that the material be either outdated or not yet covered by academic research and publications.[567] As a result, I have found that there are limitations on the amount of academic research material which is available, such as books, book chapters, reports and peer-reviewed journal articles. I would suggest that the reason for this is that the continuing development of technology creates a knowledge gap. Therefore, I have included a number of alternative resources, such as institutional databases, web-pages and news articles.

I have carried out the research by analysing a large number of documents. In order to do so, I have firstly used a top-down approach to identify the research areas relevant to address the research objectives (section 1.4). My overarching research strategy has been to collect an extensive amount of data in relation to the research areas I have identified (see keywords below). The next step has been to break down the data collected into smaller units in order to organise the data. The top-down approach has been useful for

[566] Long and Franklin (2004) ‘The paradox of implementing the government performance and results act’,309-310.
[567] Cf. Pearce et al (2010) ‘Digital scholarship considered’. EC (2007b), EC (2009b), EC (2009c), EC (2011a), EC/HREUFASP (2013).

collecting and bringing together a large amount of data from a variety of sources, and categorise it by creating a short list of relevant terms for this.[568] In order to do so, I have used a number of keywords to identify the research area, such as:

> Anticipatory governance, cooperation, cross-sectoral cooperation, cyber-security, cyber-security strategies, European cyber-policies, European cyber-security governance, risk, NATO, the Council of Europe, the European Union, public-private partnerships, transnational cooperation.

To organise the research material within this identified scope, I have primarily use a grounded theoretical approach, which enables me to select the sources and link them to the search terms outlined above. I have found that the top-down research approach tends to neglect strategic initiatives coming from other security systems and actors outside the state-centric approach. As a result, the top-down approach is difficult to use where there is no dominant policy or agency, but rather a multitude of governmental and non-governmental initiatives, governance forms and actors. Instead, I have used the grounded approach to cover these areas, which includes implementation of decentralised processes in which the members of different cooperation determine security procedures and guidelines vertically and horizontally.[569] This has led to a methodology, where I have carried out a grounded and open-ended thematic analytical research in order to establish the importance of the sources and to progress the research objectives.

4.9.2 Data collection

The sources used in this research originate from data I have collected within existing resources such as:

> Books, peer-reviewed journal articles, articles, legislations, reports, conference papers, statistics, news cuttings and web pages.

To gather data, I have used sources contained in libraries and on Internet databases, such as:

> Google, Google Scholar, Lexis Library, Westlaw, EUROPA, EUR-LEX, international organisations′ internal data archives, web pages, and news cutting.

The research covers academic publications, public policies, international conventions, legislation, frameworks, action plans and roadmaps. To organise the material, I have divided the documents gathered into four groups depending on the type of source. These

[568] Sabatier (1986),21-48. Cf. Mazmanian and Sabatier (1983) *Implementation and public policy*. Mazmanian and Sabatier (1989) *Implementation and public policy*. Matland (1995),145-174.
[569] Charmaz (2014),14. Cf. Healy and Perry (2000). Glaser and Strauss (2009).

categories include legal and policy documents, private sector/business documents, media materials used in a grounded approach. I have explored the research objectives by narrowing down the research to one particular field of security rather than focusing on the broad interpretation of security and current policies. As a result, the present study employs law, policy-making, social and political scientific sources to undertake the data collection (keywords outlined in appendix 2).

4.9.3 Analysing Significant Anticipatory Governance Structures

The findings in this research are transferred to three overarching groups, which lead to a broad analysis of their coverage, the understanding of them and their use in relation to cyber-security. These three areas are identified as the main concepts in cyber-security: multileveled cooperation, security actors and anticipatory governance. I believe that this methodology, which combines a top-down approach with a grounded approach, gives the necessary flexibility to research fragmented areas, which have not yet been systematised (chapter 1).[570] The breakdown of data allows me to delve deeper into anticipatory governance forms. Then, in the second part, I have created a substantial analysis of two distinct case studies (section 4.9).

In part two, the discussion is based on objective and substantive arguments, where I discuss my critical understanding of the area deriving from the documents. I divide the analysis into smaller parts that follow the model from the section above (section 4.8, figure 8), where my analysis covers the role of the actors, nodal cooperation, and the use of anticipatory governance. The outcomes of the study are highlighted in the concluding chapter, which also contains my reflections on the findings as well as future research questions. The findings in this part are outlined in chapter 7, where I conclude on the research.

4.10 Conclusion

To utilise the cyber-security structure, I have used two security schools and their critical approach to discussing problems with current cyber-security strategies. I have chosen these two security perspectives because they cover different aspects of the security agenda; the Copenhagen School criticises state-centric security, while the Paris School is concerned with the application of governmentality done by numerous security actors. Therefore, both of these schools have a significant influence on the understanding of the cyber-security framework. The academics from the Copenhagen School bases their

[570] Charmaz (2014),13.

security approach on threats to the survival of a given referent object, which require exceptional measures. Yet, the rethinking of securitization in the Internet age adds an interesting dimension to cyber-security, which creates a foundation for the following discussion. However, in this thesis, the main argument is that the cyber-security is not only about the state; other actors are involved in the processes that bring it outside the realm of the state-centric approach. The Paris School investigates security procedures and practices developed by the security actors within the ordinary sphere, which I find more compatible with the current interpretation of cyber-security. In this context, the Paris School captures both collective and individual security and, therefore, the security approach is freed from the traditional state-centric approach. However, it is not broad enough to cover the widespread number of security actors beyond the professional security actors, as the cyber-security framework spans from states to individuals working together in constant changing formations. The constant focus on different security actors and techniques enhances the usefulness of nodal security structures, and the inclusion of governmentality makes the security perspective of the Paris School more prominent than the Copenhagen School. However, the two different perspectives and analytical frameworks makes them both useful to draw out significant features and sharpen the critique of the use of anticipatory governance and practices in the European region.

This chapter concludes the theoretical part of this thesis by outlining essential features, which influence the following discussion in part two. This study addresses the research question concerning cooperation and European cyber-security governance and practices. The aim is not to discuss all forms of security governance, but limit the discussion to overarching cyber-security strategies. Therefore, I have positioned anticipatory governance centrally, which includes resilience, prevention and preparedness as the preferred tools in the ongoing security cycle (section 3.7). The principal argument of this thesis is that changes are made to security governance and as a result, nodal governmentality takes priority to the state-centric approach, because the traditional security structure has proven inadequate to embrace the fragmented and complex nature of cyber-security. Through interaction in security-nodes, the actors develop specific rules, practices and processes that can maximise state regulation, technical regulation, awareness-raising, and education within their particular area.

PART TWO: THE CASE STUDIES: CYBER-SECURITY AND CYBER-TERRORISM

5 European Cyber-security Governance

5.1 Introduction

This part of the thesis, gives distinctive insights into concrete emerging security risks, such as cyber-security and cyber-terrorism by looking at anticipatory governance forms developed in the European region (chapters 5 and 6). Both the Council of Europe (CoE) and North-Atlantic Treaty Organization (NATO) have developed cyber-security strategies and measures. However, the European Union (the EU) has established the most comprehensive cyber-security structure compared with other institutions. This structure takes precedence in the discussion because the initiatives cover numerous security fields and reposes, which are institutionalised and imposed on different levels in the region. As stated in chapter one, I have examined cyber-security from a strategic position and leave out the operational level. Therefore, I refrain from discussing how these strategies are operationalised, i.e. whether there is a difference between the strategic and the operational levels. Moreover, the usefulness of the future-oriented approach is not included in my research, as cyber-issues issues are only visible when anticipatory governance fails to counter the risks – not if a cyber-risk is prevented.

I have based the analysis on the theoretical work discussed in the earlier chapters, which is deployed and evaluated in my case study data. My perspective, for discussing the two case studies was established in the previous chapter, when I introduced two security schools, the Copenhagen School and the Paris School, which I have used to utilise and critique the existing framework. These two schools enabled me to get insight into the different anticipatory governance forms included in cyber-security. In chapter 5, I have discussed the overarching concept of cyber-security, which covers the umbrella term for various types of online crimes (part one). In the chapter 6, I have separated cyber-terrorism from the concept of cyber-security. In this context, I have investigated particular governance forms. In these two research areas, I have examined documentary evidence, such as security strategies, communications, action plans and road maps.

In chapter 5, I examine a range of governance practices and processes considered appropriate and efficient responses to cyber-risks in order to enhance the understanding of European cyber governance. My theoretical perspective, for discussing and understanding cyber-security, is based on a particular way of seeing the governance as a part of the nodal and anticipatory governance concepts (chapter 3). As a result, the analysis follows the cyber-security framework explained in chapter 4. This introduces the particular governance areas, which utilise the discussion regarding responses to emerging cyber-risks. In this context, I investigate this security concern from a general perspective to establish an understanding of this complex area, which is both ambiguous and fragmented. Secondly, I examine the extended use of hybrid cooperation in anticipatory governance, e.g. transnational and cross-sectoral. Finally, I discuss the development of rules, practices and processes as a part of the anticipatory governance. This analytical approach entails four sub-categories, e.g. governmental regulation, technical regulation, awareness-raising, and education, and self-regulation and self-defence, which are areas identified in the documentary analysis.

5.2 The Emerging Risk of Cyber-crime

The rapidly growing dependency of cyber-space and the Internet are considered to be 'good' in society, but it also creates a paradox, because technological advances can be turned against the computer users. Thereby, it reveals a dangerous side, where the computer interconnectivity can be an easy route to 'bads' (section 3.4). The EU has established the European Cybercrime Centre (EC3) as the focal point in the EU to manage the growing number of illegal activities in this area.[571] This centre highlight that cyber-related crimes represent considerable challenges for the law enforcement agencies. To illustrate this point, the EC3 claims that the total cost of cyber-crime to society is significant, with a recent report suggesting that the loss is around €290 billion each year worldwide. This makes illegal online activities more profitable than the global trade in marijuana, cocaine, and heroin combined.[572] A Europol report, Threat Assessment (Abridged) Internet Facilitated Organised Crime IOCTA (2011), confirms the trend and stresses that this development is likely to continue due to the increasing dependency on computer and communication systems: [573]

> "As the globalisation of markets further accelerates – with an increasing number of international virtual economies – there will be more data to compromise, with a higher impact, particularly for those developing economies which will depend on globalisation and connectivity to thrive".[574]

The Europol report concludes:

[571] EC3 (2014A) 'A Collective response to cybercrime'.
[572] Europol (2013a) 'Cybercrime: A growing global problem'.
[573] Europol (2011c) 'Threat assessment (Abridged) Internet facilitated organised crime',10.
[574] Europol (2011c),10.

> “The global reach of the Internet, its networked processing power, and its provision of instant communication and data transfer technologies combine to create an environment in which every one of these 320 million citizens may fall victim to criminal activity from anywhere on the planet. In short, the Internet eliminates distance, bringing the general public and Organised Crime activity into close proximity, and eroding the distinction between internal and external threats”.[575]

These reports outline some statistics regarding cyber-crime, but it is impossible to get a precise overview due to the problem of underreporting cyber-attacks (chapter 2). Additionally, the European Network and Information Security Agency (ENISA) has published an overview of current and emerging trends in cyber-crime, which I have attached in appendix 3.[576]

The UN Convention against Transnational Organized Crime covers some of the cyber-related crimes, but it only has relevance in relation to law enforcement and the judiciary in areas where groups carry out illegal activities transnationally.[577] As a result, this Convention cannot be extended to cover individual hackers, and this is inadequate because most unlawful activities in/ through cyber-space are carried out by individuals rather than by organised groups.[578] Europol correctly states this in its Threat-Assessment (2011). This document pinpoints, for example, the important fact that cyber criminals are different from traditional ‘real-time’ criminals; they often work independently, and without a strong link to any illegal organisation. If they are somehow connected to criminal enterprises, the organisation is loosely formed and inadequate to be included in the UN Convention.[579] The nature of cyber-crime breaks the traditional profile of persons associated with the structure of organised crime and makes the traditional governance form inadequate to manage the risks:

> “The high-tech nature of cybercriminal activity results in a demographic profile not traditionally associated with transnational Organised Crime – namely, the young, highly skilled individuals who are often recruited from universities. These features find analogies in hacker culture more, where absence of hierarchy, celebration of technical proficiency and comparative youth are prevailing characteristics”.[580]

[575] Europol (2011c),11.
[576] Marinos and Sfakianakis (2012) ‘ENISA threat landscape responding to the evolving threat environment’,2.
[577] McCusker (2006),259. UN (2004b) ‘United Nations Convention against transnational organized crime and the protocols thereto’.
[578] Rahman (2012) ‘Legal jurisdiction over malware-related crimes’,413. UN (2004b),4.
[579] Europol (2011c),6.
[580] Europol (2011c),6.

5.3 Cyber-security Cooperation and Nodal Governmentality

The limited technological knowledge and understanding of cyber-space pushes governments into policy transfers and wider forms of nodal cooperation. They are simply left behind by the speed with which technology develops and forces changes in governance. Governments and a number of public actors have significant knowledge gaps, which influence the dealings with technological issues. Understandably, these actors turn to other states and security actors for inspiration to manage cyber-risk because networked threats require a networked response.[581] Different network formations develop extensive and comprehensive forms of nodal cooperation to overcome problems of governing cyber-risks. These networks can expand the reach of regulation, build trust and cooperation among actors, facilitate information sharing and establish standards of practice and performance.[582] However, in this part of the thesis, I investigate whether this is the reality of cooperation.

In the rethinking of securitization in cyber-security, every-day practices are included in the framework (section 4.5).[583] However, the Copenhagen School fails to incorporate the problem coherently in relation to the core problem of cyber-security, where a number of actors take responsibility to solve emerging online problems. Their use of everyday practices concerns very limited participation, where individuals are restricted to passing on information. I think that the use of these practices is less convincing, because the nodes are based on a large group of different participants who aim to maximise cyber-security by preventing the risks from transforming. According to the cyber-securitization approach, individuals cannot be security actors in their own right, nor can they directly decide governance forms, or mandate an active role on their initiative. There is an intense mistrust of the ability of individual users to improve their personal security, and their involvement creates a paradox, which is not visible in the Paris School′s open-ended cyber-security approach (section 4.6). This mistrust becomes very evident in the way the Copenhagen School views individuals as a liability and a threat that can create problems themselves. For example, individuals can create problems by downloading copyright protected material, contracting computer viruses or facilitating a security breach.[584] The Paris School takes a different approach by focusing

[581] Deibert and Crete-Nishihata (2013) ’Global governance and the spread of cyberspace controls’,350. Slaughter (2004) *A new world order*. Ansell et al (2012) The promise and challenge of global network governance.
[582] Beken and Verfaille (2010) ‘Assessing European futures in an age of reflexive security’,188.
[583] Hansen and Nissenbaum (2009),1165. Garcia and Palhares (2014),276–277.
[584] Hansen and Nissenbaum (2009),1166.

on everyday practices and governance forms developed through collective social groupings – in particular between security professionals. This marks a shift away from the traditional hierarchical authoritative meaning of state-centric security. As a result, the security approach includes interconnected systems in a heterogeneous structure, in which new types of spaces are developed.[585] I think that the Paris School has a more realistic perspective of the risk management of cyber-risks because of their inclusion of numerous actors in hybrid networks.

Networked cooperation is claimed to offer a flexible and relatively fast way to develop governance forms, coordinate, and harmonise national cyber-security responses while initiating and monitoring the different solutions to cyber-security problems.[586] The Paris School decentralises the state by focusing on several professional security actors, such as individual actors, institutions and networks of the security professionals. These actors are all involved in the process and have a significant role to play in securing cyber-space (section 4.6). It is true, that states, groups and individuals can claim ownership over fragmented areas of cyber-space. However, the sovereignty only relates to a particular part of its material infrastructure, or it will relate to the possibility to opt out of it entirely. Yet, I would argue that it is impossible to securitize this area. For example, the Heartbleed bug (2014) that attacked web-servers running OpenSSL worldwide.[587] Exceptional measures can be put in place, and for a short time, it is possible to shut down OpenSSL by securitizing a limited number of computer technologies related to the server. However, managing global threats require consensus among security actors and shared strategies instead of attempting to securitize an issue worldwide, which will have no effect unless all possible users frame it in the same way. This argument disadvantages the state-centric and elitist perspective of the securitization theory. Even though, the updated version includes more actors than previously, it fails to accommodate the multi-levelled approaches incorporated in anticipatory governance (chapters 3 to 6).

A range of initiatives in Europe is introduced to make the governance of cyber-space more efficient. This signifies that cooperative formations are required to manage differentiated security approaches with numerous security actors, i.e. Internet users and user groups, network infrastructure providers, corporate security organisations, non-

[585] Radu (2014),8.
[586] Slaughter (2004),317-318.
[587] Hearn (2014).

governmental and governmental organisations, etc.[588] I think that the real problem derives from extensive use of these hybrids, which has created a complicated structure. It is problematic that all initiatives are fragmented and therefore, they are developed parallel to other networks with limited, if any, collaboration between the initiatives and the actors. Moreover, the progress is not reported widely in the system. This is one of the major problems in cyber-security, and this will continue as the structure continuously expands, because most crimes in ’reality’ have links to cyber-space.

The EU highlights that it is the responsibility of all relevant stakeholders to be involved in cyber-security. As an example, the joint Communication (2013) states that the responsibility for a more secure cyber-space lies with all players in the global information society, from citizens to governments:

> “The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities that need to be properly defined, thoroughly analysed, remedied or reduced. All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity”.[589]

This requires that all relevant stakeholders define norms of behaviour in cyber-space, respect rules and existing laws. The EU encourages actors to develop confidence-building measures, to increase transparency, and reduce the risk of misperceptions in state behaviour, and this is a challenge to security actors.[590] Because of Snowden’s revelations, the role of states and their cooperation are under public scrutiny.[591] This has resulted in changes in the security perception, generating a move away from the secrecy included in previous policies and approached. This includes more oversight and accountability in future governance. The absence of proper oversight mechanism creates a vacuum for security actors to develop exceptional measures beyond the original mandate (sections 5.7, 6.7). I think that the requirement for more accountability and transparency versus secrecy of strategic and operational governance has created a double-edge sword for the security actors. Secrecy has a legitimate basis when fundamental national interests are at stake. However, secrecy has sometimes been used

[588] Wall (2007a),211.
[589] EC/HREUFASP (2013),4.
[590] EC/HREUFASP (2013),15.
[591] The Guardian (2013/2014) *The NSA files.*

to suppress public debate and conceals information, and this generates mistrust among the public.[592]

5.4 Transnational Cooperation

There is a strong consensus about the historical development and the use of cooperation. Firstly, there are significant movements away from the traditional state-centric approach towards an open-ended form of security governance created in nodes (sections 2.3, 2.4). Secondly, these nodes develop their own procedure of self-governance to manage the security issue by developing anticipatory governance and practices (section 3.7). The most used form of cooperation is linked to transnational collaboration between states and state actors. It does not signify that they alone make the decision; they might bring in experts or participants from the private sector in different areas. However, there is still a visible division between internal-external security and public-private participation in the cyber-security policies. On the surface, this contradicts the Paris School's claims that contemporary security governance merger together the different security dimension in a complex structure.[593] The cyber-strategies set out directions within the EU, NATO and CoE, which appear fundamentally state-centric. It is visible that state actors decide on cyber-security, but they are not kept entirely on closed cooperative systems. I have identified that the public actors reach out to international actors, organisations and businesses to be involved. Therefore, the actual development of governance and practices breaks the state-centric phenomena and indirectly mergers the different security dimensions, i.e. internal-external and public-private security (chapter 3).

European institutions and organisations have cyber-security positioned high on their security agenda. The CoE developed The Convention on Cyber-crime in 2004, with the purpose of ensuring that the Internet provides a safe and open environment where freedom of expression, freedom of assembly, diversity, culture, education and knowledge can flourish.[594] NATO has developed its cyber-security over the last decade, and its cyber defence policy and the associated action plan creates a clear vision of how the alliance plans to bolster its efforts.[595] Finally, the EU has developed an extensive range of rules, processes and practices for its Member States in order to harmonise and improve cyber-security and to ensure a free and safe Internet. Cyber-security falls under

[592] Lin and Dam (1996) 'Preference',XIV.
[593] Salter (2008a),247.
[594] CoE (2014b) 'Cyber-crime. A threat to democracy, human rights and the rule of law'. CoE (2014e) 'The Council of Europe and the Internet. Freedom and safety online'.
[595] NATO (2014) 'NATO and cyber defence'.

the scope of the Area of Freedom, Security and Justice. The background for the security initiatives are outlined in the Lisbon Treaty (2007),[596] the Stockholm Programme (2010),[597] and the Action Plan to implement the Stockholm Programme (2010).[598]

5.4.1 International Cooperation

The UN acknowledges that an adequate protection requires communication and cooperation between all stakeholders. Therefore, the organisation encourages all relevant parties to develop security strategies to counter cyber-crime and to enhance the protection of CIIs.[599] It is perhaps surprising then that the organisation itself has failed to develop a comprehensive global cyber-security convention, with the latest proposal for a global treaty being rejected by Russia, China and a number of developing countries in 2010.[600] The lack of a globally supported agreement is arguably the most significant obstacle to manage cyber-risks. The absence of a universal consensus creates a negative complexity spiral where numerous initiatives, guidelines, practices are developed in a very complicated system involving states, businesses, groups and individuals worldwide.

There is a reason for the reluctance of some countries to agree on treaties and conventions, which binds them. Major cyber-espionage networks and cyber-attacks have been linked to China, Russia and other countries, who benefit from these activities. Therefore, these countries have introduced little or partially symbolic measure against hackers because of the strategic benefits they offer in obtaining information. This reveals the ineffectiveness of the cyber-responses when hackers can receive protection in some countries.[601] However, the unwillingness for developing definitions and governance practices creates a vulnerable position for these states too, as there is a high risk for retaliation after a cyber-attack. The alleged North Korean cyber-attacks against Sony Entertainment in 2014 highlights the problems regarding the vulnerability of both states and businesses, as well as investigative and law enforcements concerns, because there was no clear proof that North Korea had actually carried out the attacks. Yet, the

[596] EU (2007) 'Treaty of Lisbon amending the treaty on European Union and the treaty establishing the European Community'.

[597] EC (2010j),22-23.

[598] EC (2010e),36-37.

[599] UN (2004a) 'Creation of a global culture of cybersecurity and the protection of critical information infrastructures',2.

[600] Masters (2010) 'Global Cybercrime Treaty Rejected at U.N.',1.

[601] Deibert and Crete-Nishihata (2013),353.

situation is framed by the mass media and the U.S. that North Korea was the perpetrators (section 1.1).[602]

Cyber-security creates a challenge for all security actors, and this supports my claim that widespread governance formations are needed that enable security actors to work together. The involvement of non-governmental actors does not only relate to international security organisations. It has another dimension, where organisations, corporations, businesses, groups and individuals on multiple levels can discuss and develop proactive measures through cross-sectoral cooperation. Several organisations have tried to develop different forms of cooperation. The UN strongly emphasises the promotion of PPPs to share and analyse information concerning CI to prevent, investigate and respond to damage or attacks on vulnerable areas.[603] The G8 has also explicitly focused on cooperation between sectors. During the Paris Cyber-crime Conference (2000), a co-regulation on the Internet between governments and private high-tech businesses was proposed as a solution to the emerging problem of managing the Internet. The proposals failed to gain support from the industry because they feared that governmental initiatives would lead to enhanced control.[604] I find this negative attitude of mistrust significantly damaging, and it prevents creating anticipatory governance plans because the actors put self-interest first. As a result, they simply fail to recognise the urgency of developing a shared approach (sections 3.3.2, 4.8.2).[605]

The EU's cyber-security strategies focus on dialogue with like-minded countries from outside the EU. The underpinning reason, for expanding the security network, is to achieve a high-level of data protection that also includes the transfer of data to countries outside of the EU, because globalisation has made it impossible to exclude the global dimension. In the EU Communication (2009) on critical information infrastructure, the objectives are to archive consensus on the European priorities for the resilience and stability of the Internet at both the strategic level and the operational level. The aim is to improve resilience and preparedness by incorporating them into dialog and cooperation with the global community, i.e. none-EU countries, and international organisations.[606] This is supported by the joint Communication (2013):

[602] Zetter (2014) 'Sony got hacked hard'.
[603] UN (2004a),2.
[604] G8 (2000) 'G8 conference on cybercrime'.
[605] EC (2013d) Measures to ensure a high common level of network and information security across the union',3.
[606] EC (2009b),7.

> “The responsibility for a more secure cyberspace lies with all players of the global information society, from citizens to governments. The EU supports the efforts to define norms of behaviour in cyberspace that all stakeholders should adhere to. Just as the EU expects citizens to respect civic duties, social responsibilities and laws online, so should states abide by norms and existing laws. On matters of international security, the EU encourages the development of confidence building measures in cybersecurity, to increase transparency and reduce the risk of misperceptions in state behaviour”.[607]

The cooperative network goes beyond neighbouring countries; the EU seeks to establish close cooperation with other security organisations, such as the CoE, OECD, UN, OSCE, NATO, AU, ASEAN and OAS.[608] From my own nodal security perspective, transnational cooperation constitutes a necessary supplement to the traditional state-to-state cooperation, as these have a certain level of specialised knowledge useful for governing the area. Moreover, the use of technical experts can replace the traditional speech-act actor to obtain the legitimacy for developing exceptional measures in a state or institutional frame (section 4.5.3).[609] It is likely to have security experts actively involved in developing anticipatory governance and practices as part of a contract with state actors, or as an equal part of a private-public partnership (PPPs). This circumvents the inclusion of actors in Nissenbaum and Hansen’s technification. Nevertheless, this broad foundation of different actors adds to the complexity of cyber-security governance, which creates obstacles in establishing a sufficient overview and to measuring the success rates of these initiatives.

Outside the different treaty systems, agreements are reached to enhance cooperation between countries. Through bilateral agreement, cooperation with the United States has been established. This will be further developed, notably in the context of the EU-US Working Group on Cyber-security and Cyber-crime.[610] Moreover, bilateral and multilateral agreements and dialogues are in place with international organisations. The EU, for example, has established cooperation with the ITU, the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF).[611] The inclusion of actors outside the state-system breaches the stronghold of the state-centric arguments forwarded by Copenhagen School. More importantly, it supports the Paris School’s perspective of deepening the security agenda with multi-levelled cooperation of every-

[607] EC/HREUFASP (2013),15.
[608] EC/HREUFASP (2013),15.
[609] Buzan et al (1998),23-24. Hansen and Nissenbaum (2009),1157. Garcia and Palhares (2014),275-277.
[610] EC/HREUFASP (2013),15.
[611] EC (2013d),6.

day practices (chapter 4). However, the side-effects are that cooperation becomes increasingly complex and fragmented. Unfortunately, the demand for more cyber-security overshadows the requirement of more transparency and accountability (appendix 8). The EU supports this enhanced cyber-security framework. In the EU Communication (2009), the document pinpoints two important areas, i.e. common consensus, and engagement beyond the region:

> “First, achieving a common consensus on the European priorities for the resilience and stability of the Internet, in terms of public policy and of operational deployment. Secondly, engaging the global community to develop a set of principles, reflecting European core values, for Internet resilience and stability, in the framework of our strategic dialogue and cooperation with third countries and international organisations”.[612]

5.4.2 The Council of Europe and the Convention on Cyber-crime

At the forefront of the different cyber-security initiatives are the CoE’s Convention on Cyber-crime.[613] The preamble outlines that the CoE recognises the value of fostering cooperation with other states. Nevertheless, this Convention is a product of its time, which was developed when the problem of cyber-crime was finally recognised. I would argue that the Convention fails to encompass all three sub-units included in cyber-security. Firstly, cyber-warfare and cyber-terrorism are not covered similarly to cyber-crime in existing legislation. Therefore, it is necessary to create an analogue from cyber-crime offences. Secondly, this Convention does not include cooperation on the horizontal level as it fails to recognise the usefulness of having businesses, corporations, groups and individuals listed in the framework. Although, the Convention reaches out to private industry, it is still a state-centric framework, where the signatory states are fully in charge of decision-making to manage cyber-risks.

This view is similar to the Copenhagen School’s perspective by including only a limited group of security actors, despite being open to cooperate with private industry. Yet, the Paris School, who do not see the state as the sole provider of security, rightly contests this approach (section 4.6). Accordingly, I believe that these limitations damage cyber-security as the present framework includes a variety of actors, directions and criminal activities, which remain unaccounted for by the convention. By only depending on public security actors to cooperate in a transnational network, the convention establishes a one-dimensional governance form that is not up-to-date with the current threat level.

[612] EC (2009b),7.
[613] CoE (2013b) ‘Who we are’.

In the European region, the CoE Convention still has a purpose, despite being outdated in some areas. Nevertheless, the Convention lacks commitment from the wider international community, with only 53 states having signed up for it, and 44 states who have ratified it, as well as 2 CoE members who have not signed up to it (January 2015).[614] I find this concerning because it is commonly acknowledged that an international treaty is needed to harmonise the effort and create consensus. However, I would argue that if a large number of states reject to sign up and ratify the treaty, the Convention has limited value in the global fight against cyber-crime, and other alternative governance forms takes precedence. I am not particularly surprised to find that Russia stands outside the CoE's cyber framework, just as Russia has objected to the UN Treaty.[615] There are different reasons for the general lack of commitment. Different countries have different priorities; some do recognise that particular forms of regulation are needed, and others do not recognise cyber-offences and regard them as falling under the scope of existing laws. Given the technological, legal and cultural diversity of the world's nations, the risk perception differs significantly (section 3.6.1).[616] Because of the different perceptions of cyber-risks worldwide, I believe that the possibility of determining a joint strategy is close to 'mission impossible'.

5.4.3 The EU and Regional Cyber-crime Cooperation

The EU recognises the need for transnational cooperation to manage cyber-risks. The agreements involve developing preventive and precautionary instruments, developing technical measures, exchanging knowledge, education, and harmonising law enforcement mechanisms.[617] This need for cooperation is highlighted in numerous EU communications (appendix 8).[618] The Paris School has argued that the internal and external dimension is no longer clear-cut. However, I argue that the problem regarding internal cooperation needs to be addressed to create a more coherent approach to increasing resilience and preparedness (section 3.7). The internal market and cooperation between the Member States are core elements of the EU. Therefore, the internal aspect of cyber-security is paramount for developing an anticipatory structure. If the Member States fail to cooperate in an area which effect economic, political and social life of the union, how can they be taken serious as a security actor externally?

[614] CoE (2015) 'Convention on Cybercrime. Status'.

[615] *In July 2013 the United States and Russia signed an agreement in order to reduce the risk of conflict in cyberspace through real-time communications about incidents of national security concern.* Nakashima (2013) 'U.S. and Russia sign pact to create communication link on cyber security'.

[616] Grabosky (2007b),207.

[617] Wall (2007a),211.

[618] EC (2007b),5. EC (2009c),6-7. EC (2011a),6. EC/HREUFASP (2013),3.

The EU 2005 Decision regarding protection against cyber-attacks was quickly outdated.[619] In 2013, its successor was finally adopted. This new piece of legislation took three years to be adopted from its first draft which was presented in 2010.[620] This slow legislative process opens up the opportunity for security actors to create their own anticipatory governance forms and practices because a coherent legal guideline is missing. Instead, the development is left in the hands of security professionals who routinely develop governance forms without interference or public scrutiny. This is understandably an area that the Paris School criticises because it gives security actors free reign to advance their interpretation of security without an appropriate control system. I side with the Paris School's critique of the complicated nodal system and the power transferred to the security actors. It is evident that the nodal system is a victim of its own success. The nodal structure is needed to manage the diversity of cyber-risks (section. 4.6.4). On the contrary, its complexity hinders and obscures transparency, and it is simply impossible to get an overview of the different processes and procedures in place. Within the EU system, the Lisbon Treaty closed a number of legal gaps by rendering agencies and other bodies subject to judicial review and thereby bringing the area within the power of legal accountability.[621] Despite this improvement, I believe that cyber-security is surrounded by a high level of secrecy, and the judicial review has a limited effect as most strategies are kept within a defined group of actors.

The 2013 EU Directive addresses more security issues in the use of the Internet than previously.[622] However, to close new legislative lacunas, a new Directive proposal (2013) Measures to Ensure a High Common Level of Network and Information Security across the Union has been launched to improve security of the Internet, private networks and information systems.[623] Importantly, when this Directive is adopted, it covers Member States, international cooperation and private stakeholders to ensure effective collaboration in relation to all crime types included in cyber-security.[624] Again, it is visible that the EU aims to open up the security framework and include a growing number of stakeholders. This goes beyond the rethinking of the securitization approach, because it is not only technical experts who are included in security governance.[625]

[619] EU (2005) 'Attack against information systems'.
[620] Global Organizations (2014) 'EU Law'.
[621] Craig (2010),115.
[622] EU (2013) 'Attacks against information systems and replacing Council Framework Decision 2005/222/JHA',6.
[623] EC (2013d),3.
[624] EC (2013d).
[625] Hansen and Nissenbaum (2009),1157. Garcia and Palhares (2014),275-277.

However, the problem with all these good intentions and progressive initiatives is that they are drowned in bureaucracy and hierarchical structures that cannot deploy flexible and alternative measures, and it ends in something normatively attractive but not really functional in reality.

The ultimate deadlock of processing anticipatory governance forms is linked to the paradox of uncertainty and decision-making, where no-one knows if the risk will develop. Still, decisions need to be taken to create obstacles without actually knowing the effect of them (section 3.6).[626] There is no success criterion that it can be measured against, and there are no statistics available which show the number of risks that has been prevented. Therefore, the decision-makers rely on imaginative scenarios without knowing if it actually makes any difference. Yet, the long process of developing and harmonising legislation creates a situation where the likelihood of the risks develops unhindered in the legislative lacuna. I maintain the argument, that the slow process of regulation through law creates unnecessary problems when it is progressed through a substantial bureaucratic structure. It is clear that the whole process suffers from 'the problems of many hands', where policies pass through a large number of hands before they are adopted and implemented.[627] Directives, decisions and communications are often the results of numerous committees, where members, administrative bodies and departments conform to the traditional rules and existing practices - and sometimes they contribute to ideas and rules.[628]

To address the legislative gap, the EU introduced a number of communications. The 2007 Communication correctly outlines significant problems regarding the fight against cyber-crime:

> "The lack or underutilisation, of immediate structures for cross-border operational cooperation remains a major weakness in the area of Justice, Freedom and Security. Traditional mutual assistance when confronted with urgent cybercrime cases has proven slow and ineffective, and new cooperation structures have not yet been sufficiently developed."[629]

The 2009 Communication states, for example, that the problem concerning cooperation remains unsolved:

[626] Beck (1999) World risk society,78. Mythen and Kamruzzaman (2010) 'Counter-terrorism and community relations',219.

[627] Bovens (2007),457. Thompson (1980) 'Moral responsibility of public officials',905. Cf. Bovens (1998) *The quest for responsibility*.

[628] Bovens (2007),457-458

[629] EC (2007b),6.

> "A purely national approach runs the risk of producing a fragmentation and inefficiency across Europe. Differences in national approaches and the lack of systematic cross-border cooperation substantially reduce the effectiveness of domestic countermeasures, inter alia because, due to the interconnectedness of CIIs, a low level of security and resilience of CIIs in a country has the potential to increase vulnerabilities and risks in other ones".[630]

Still, Member States are improving their security framework by updating their existing framework. For example, Denmark is preparing a new cyber-security strategy. The Czech Republic and Estonia are updating their national policy. Lithuania is in the final stages of the policy design and finally, the UK has published a survey (2014) on information security breaches within their national cyber-security strategy framework.[631] However, it is impossible to know if these countries have made use of existing guidelines to draft their national strategies. If not, these updates will add to the difficulties in finding a harmonised approach.

It is clear that bureaucratic legislative processes are a significant part of the weaknesses of the cyber-security structure. Considering that this is a complicated area, and that technology changes have improved rapidly beyond everyone's imagination, it is still noteworthy that there is a standstill, which creates a legislative lacuna in the cyber-security framework. Thereby, it gives hackers an advanced position. Despite the different initiatives in the EU to maximize security, the Member States remain slightly reluctant to harmonise and develop collective management structures. Even though countries have democratically decided to become members of the EU, it does not signify that they have a shared identity – nor does it signify that they share the same values. Because the Member States have different legal systems and constitutional arrangements, it has proven difficult to make a uniform approach to enhance resilience against cyber-attacks.[632] I believe that this issue is an important, but ongoing problem, because the bureaucratic structure is too heavy, and the unwillingness of the Member States to develop and/or harmonise legislative and governance structures hinders the introduction of a more comprehensive framework. Changes have been made because of these claims, and special security agencies have overtaken some of the responsibility to enhance resilience and create responses to cyber-risks, i.e. European Network and Information Security Agency (ENISA) and EC3.[633] Yet, these changes are not radical

[630] EC (2009b),5.
[631] ENISA (2014c) 'News on national cyber security strategies in the European Union and worldwide'
[632] Neal. Andrew W. (2012b) 'Terrorism, lawmaking, and democratic politics',358.
[633] Craig. Paul (2010) *The Lisbon Treaty*,114.

enough to accommodate the need for a more flexible structure which is free of the traditional bureaucratic strings.

5.5 Cross-sectoral Cooperation in the European Region

The involvement of multiple actors represents a move away from a purely public-based security management form, which mostly signifies that the state-centric governance form is incompatible with the nodal governance structure. However, the vast majority of incidents are manufactured and caused because of weaknesses in the computer-systems (section 3.6). Both the public and the private sectors acknowledge their vulnerability towards these events, which can stop states and businesses from functioning and generate financial losses.[634] It is clear that there is an ongoing threat towards given referent objects, which justifies the expansion of the securitization perspective to consider cyber-security as the sixth sector for cyber-security (section 4.5).[635] However, from my security perspective, cyber-security is not about developing threat-based security policies, because the problem does not concern 'waiting for threats to materialize'.[636] Instead, I would argue that it is about preventing the risk from transforming, and this stance includes a large group of security actors because cyber-security concerns everyone who uses computer technologies in everyday life.

Security experts are not necessarily state actors or security professionals in a particular area. The scope of security actors is much bigger and covers groups and individuals with special knowledge to counter the risks. In cyber-security, a group of individual actors are largely overlooked and kept out of the public debate, while the use of individual hackers in security cooperation is increasing. In terms of the hacker culture, ('white hats'), I recognise the usefulness of including these young and highly technical skilled people in the framework to enhance security, rather than posing a threat (section 1.1). Hackers are potentially useful because they have an extensive knowledge of new computer trends and system weaknesses, which can be transferred to developing anticipatory cyber-security measures. Otherwise, these technical skills could be potentially used to pursue a career in illegal enterprises. In the Copenhagen definition of technification, these hackers and other individual actors are not regarded as trustworthy experts (sections 4.5.2, 4.5.3). The Copenhagen School scholars argue that a privileged

[634] EC (2013h) 'Proposed directive on network and information security'. EC (2013d),2. Cf. Deibert and Rohozinski (2010b). Aradau and van Munster. (2007). Bonditti (2004) 'From territorial space to networks'. EC (2013h).
[635] Hansen and Nissenbaum (2009),1157. Garcia and Palhares (2014),275-277. Silomon and Overill (2012),15.
[636] De Goede (2008),164

role is assigned to computer and information scientist within the cyber-security discourses and this is partly a product of the logic behind the securitization itself:

> "[I]f cyber-security is so crucial it should not be left to amateurs".[637]

I contradict this argument, because the title, technical experts, is open to interpretation. It is certainly debatable who the real experts are: a 'white-hat' hacker, or a computer scientist. Through their clandestine work, hackers have a more nuanced understanding of vulnerabilities in computer systems than theoretical experts do.[638] Accordingly, hackers are often one-step ahead of the security measures through their knowledge of systems and weaknesses. However, I would argue that this constitutes a sort of, the 'chicken and the egg' paradox. To be ahead of security, gaps in computer systems or programs need to be exploited, and the activities of the hackers lead to new updates and programmes. New updates and programmes constitute new challenges to the hackers, and these continual improvements in cyber-security expand their virtual playground – and this process is set to continue.

The Paris School recognises that amateurs can play an important role in the security process by intervening and challenging the existing framework. However, the Paris academics also highlight that there is a problem related to the use of amateurs because they constantly need to prove that they have explicit and sufficient knowledge. This is different with security professionals and experts; they are trusted due to their accreditation – even though they might not be up to date with their technical knowledge. As a result, the technical experts' claims are used without demonstrating their knowledge in relation to a particular problem (section 4.6).[639] On the operational level, there seems to be a wider acceptance of using individuals. For example, a convicted LulzSec hacker got his sentence reduced because he helped the FBI prevent 300 cyber-attacks.[640] Large software companies employ certificated 'white hat' hackers to break into their own systems and root out weaknesses.[641] Microsoft has for years used so-called 'Microserfs'. These are hackers that have become co-opted into the corporate structure due to their programming and technical skills. This trend, of using 'converted'

[637] Hansen and Nissenbaum (2009),1167.
[638] Caldwell (2011) 'Ethical hackers'. Conrad (2012) 'Seeking help: the important role of ethical hackers'.
[639] Bigo (2002),74.
[640] Pilkington. (2014) 'LulzSec hacker 'Sabu' released after 'extraordinary' FBI cooperation'.
[641] Conrad (2012). Everett (2009) 'Ethics – a question of right or wrong'.

hackers in public and private sectors, is spreading, because they are often the only actors who have the skills and the curiosity to explore the gaps in security systems.[642]

5.5.1 The CoE and Cross-sectoral Cooperation

A CoE motion (2007) includes the recommendation of a political framework for cooperation against cyber-attacks. It was suggested that there is a need to go beyond the legal framework provided for in the CoE's Convention on Cyber-crime and the CoE's Convention on the Prevention of Terrorism.[643] The CoE highlights the insufficiency of the current legal framework, where a limited number of Member States have ratified the first convention. Moreover, there are gaps regarding the definition of a sovereign state's cyber-space, and the issue of cyber-terrorism.[644] The motion states, for example, that:

> "[I]t is necessary to go beyond the legal aspects, and establish an efficient political framework that provides rapid reactions against cyber-attacks and the threat posed by cyberterrorism".[645]

This introduces the idea that the cyber-security is not purely a state concern. Despite states being the only signatory parties to the existing Convention, it argues that future security policies should:

> "[F]acilitate immediate political consultations and exchange of information amongst those concerned: government authorities, parliamentarians, the private sector and experts in this field".[646]

This citation supports the Copenhagen School's inclusion of every-day practices and technification (section 4.5). Moreover, it embraces the idea that the private sector and technical/scientific experts have something the state needs because they can provide much needed information. However, despite this information flow which could improve security strategies, experts and individuals do not receive the same equal status. Accordingly, the CoE does not open up completely for PPPs as the preferred platform for cooperation - they still keep experts and business on a consultancy level. Nevertheless, they come very near to accepting that other security actors can contribute to the decision-making process, i.e. international organisations and non-CoE Member States.[647] Whether this extension, is sufficient to make any difference is debatable compared to initiatives developed by other institutions. For example, the EU accepts

[642] Jordan and Taylor (2004),12.
[643] CoE (2005a) 'The Council of Europe Convention on the prevention of terrorism'.
[644] CoE (2007b) 'A political framework for co-operation against cyber-attacks',1.
[645] CoE (2007b),1
[646] CoE (2007b),1.
[647] CoE (2007b),1. Emmers (2010),137

that they cannot manage cyber-security without including the private sector, and they have tried to accommodate this in their strategies. I can understand the reluctance to expand the framework, because the CoE is a transnational organisation founded by states, and only states can be parties to the conventions. It is, therefore, not surprising that they do not go further in adding a new structure to their existing framework. Nevertheless, I think that it is a shame that the CoE have stopped this progress halfway through, and thereby, the organisation have missed the chance to include significant security actors in the framework, who could make a difference to governing cyber-space.

5.5.2 The EU and Cross-sectoral Cooperation

The EU's Internal Security Strategy, includes indirectly, cyber-crime, where it focuses on the disruption of international crime networks, prevention of terrorism, addressing radicalisation and recruitment, strengthening of security through border management, and improving Europe's resilience to crises and disasters. The action plan highlights that nodal governance is required to improve European cyber-security. For example, it is highlighted in the strategy that:

> "Cooperation between the public and private sector must be strengthened on a European level through the European Public-Private Partnership for Resilience (EP3R). It should further develop innovation measures and instruments to improve security, including that of critical infrastructure, and resilience of network and information structure".[648]

I give cross-sectoral cooperation a significant position in the cyber-governance structure. This inclusion reduces the influence of the state-centric approach, as citizens, businesses, governments and CIs has a role to play in increasing cyber-security.[649] The same argument is incorporated in the joint EU Communication (2013) that argues that because of the growing dependencies on ICTs, vulnerabilities have increased in society. I have noticed that the rhetoric used in this communication is centred on responsibility; this marks a change from 'protection' toward a 'shared responsibility'. Thereby, it is explicitly recognised that every user has a responsibility to manage security by protecting their computer-systems and software. As a result, I think that it is impossible to limit governance to individual states and state founded organisations.[650] I would place emphasis on the argument that all computer users have a responsibility to set up

[648] EC (2010i) 'The EU internal security strategy in Action',10.

[649] EC (2010f) 'Internal security strategy for the European Union',4. Cf. EC (2010b) 'A digital agenda for Europe'. EC (2010a) 'Attacks against information systems and repealing Council Framework Decision 2005/222/JHA. Proposal',2.

[650] EC/HREUFASP (2013),4.

preventive barriers, built up resilience, and prepare continuity plans (figures 4 and 5). If cyber-security is everyone's responsibility, and everyone can be involved in governance on different levels, and I maintain that there are private experts who are eligible to be part of the framework, equally to public actors – or even beyond public security actors.

This approach is incompatible with the Copenhagen School's rethinking of securitization, technification, and everyday practices, that to some extent includes individuals (section 4.5).[651] I would also argue that it current cyber-security structure goes beyond the motion of the CoE, because of its restrictions on including security actors. The proliferation of security technologies and actors reach beyond the traditional institutions of government and the traditional route for establishing cooperation. Multi-levelled anticipatory governance is strongly linked to different security techniques, such as surveillance, profiling, risk management, data mining, biometrics and information sharing among security agencies worldwide (section 4.6.1). These technologies are essential in order to categorise and assess the risks early in the process.[652] Europol includes this perspective in their Threat Assessment, when they state:

> "There is now an urgent requirement for authorities in the EU to optimise measures to counter cyber criminality in active partnership with other sectors of society, not only drawing on their knowledge of Internet culture, Internet-facilitated criminality, and emerging technological developments with a view to anticipating criminal behaviour, but also pooling resources and expertise to deliver coordinated, high impact control measures and enforcement responses".[653]

5.5.3 The EU's Public-Private Partnerships

EU's Communication on CIIP (2009) promotes the multi-stakeholder and multi-level concept as an integral part of anticipatory governance. The communication highlights the need for a multi-levelled approach:

> "It is necessary to strengthen the existing instruments for cooperation, including ENISA, and, if necessary, create new tools. A multi-stakeholder, multi-level approach is essential, taking place at the European level while fully respecting and complementing national responsibilities".[654]

Europol supports this statement. According to Europol, there is an urgent requirement for EU authorities to optimise measures to counter cyber-criminals in active partnership with other sectors of society. It is not enough to draw on their knowledge of Internet

[651] Hansen and Nissenbaum (2009),1157. Garcia and Palhares (2014),275-277.
[652] Neal (2012a),263. Bigo (2008a).
[653] Europol (2011c),11.
[654] EC (2009b),7.

culture, Internet-facilitated criminality and emerging technological developments with a view to anticipating criminal behaviour. Instead, it is necessary that the different sectors pool resources and expertise to deliver coordinated, high-impact control measures and enforcement responses.[655]

Compared with other regional security organisations, the EU has developed a sophisticated network of cross-sectoral cooperation. An example of cross-sectoral cooperation is the newly established EC3 (2012), which includes a variety of actors, such as EU Member States, key EU stakeholders, non-EU countries, international organisations, Internet governance bodies, service providers, companies, academic experts, civil society groups, National Computer Emergency Response Teams (CERTs), and the CERT-EU.[656] Moreover, formalised European PPPs are developed to improve the resilience of attacks against CII and ICTs. PPPs are already established, and were created by the European public-private Partnership for Resilience (EP3R) as a model for the first formalised partnership in cyber-security. The use of equal partnerships is extended to an EU-US PPP (chapter 6) and the Network and Security Public-Private Platform (NIS PPP).[657] The NIS PPP is the latest partnership established to manage cyber-crime (2013). This project is interesting as it extends the scope to cover all aspects of network and information security, whereas EP3R is only related to CII.[658] This PPP aims to bring together relevant public and private stakeholders, to identify good cyber-security practices across the sectors and to create favourable market conditions for developing and adopting functional security measures that increase resilience.[659] The most remarkable aspect is the inbuilt deadline, which highlights a change in the understanding of the urgency to develop governance forms:[660]

> "The output of the platform will feed into the Commission recommendations on cybersecurity across the value chain to be adopted in 2014, as well as the implementation of the risk management and incident reporting obligations under the proposed NIS Directive".[661]

This statement promotes politically and normatively sound values concerning information sharing. Unfortunately, these nodal cooperation show a different reality,

[655] Europol (2011c),11.

[656] Europol (2013d) 'Joining forces to catch the criminals'.

[657] EC (2010g) 'EU-U.S. Summit 20 November 2010'. EC (2010d) 'Cyber Security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats'. EC (2013e) 'NIS public-private platform'.

[658] EC (2013e).

[659] EC (2013e).

[660] EC (2013e).

[661] EC (2013e).

where problems relate to the lack of output in the public sphere (section 6.6). Valuable information and outcomes are often kept inside the nodes rather than being communicated to a larger audience. After examining various EU Communications, web-pages and published material concerning these security nodes, I still find it impossible to identify who are involved, the structure, the aims, the scope and the outcomes. From my own security understanding, this lack of communication does not promote transparency in a complex area, nor does it encourage security actors to participate in any cooperation. Accordingly, other security actors will miss out valuable information that affects their own particular security problem.

5.5.4 Engaging Public and Private Sectors

The discussion above provides evidence of the rising awareness among security actors of the need to include none-governmental actors in the nodal structure. This undoubtedly demonstrates the requirement of a three-dimensional framework to manage the anticipatory cyber-risks, i.e. national, transnational and cross-sectoral cooperation (sections 3.6, 3.7). The differences between former threat-based policies and strategies and anticipatory cyber-security strategies are linked to the explicit use of public and private actors. The distinction is based on the state-centric approach used in threat-based strategies, where the public-private dimension is absent (the Copenhagen School). The combination of both transnational cooperation and cross-sectoral cooperation are placed equally in the cyber-security framework, and the involvement of both areas gives a more comprehensive response to cyber-risks. This is part of the national state and the state-centric approach, which sidelines more traditional security governance. For example, the joint Communication (2013) makes the link between these actors, who are not traditionally associated with security. The Communication claims that is it important to:

> "[I]mprove preparedness and engagement of the private sector. Since the large majority of network and information systems are privately owned and operated, improving engagement with the private sector to foster cybersecurity is crucial. The private sector should develop, at technical level, its own cyber resilience capacities and share best practices across sectors. The tools developed by industry to respond to incidents identify causes and conduct forensic investigations should also benefit the public sector".[662]

The nodal governance, of course, involves an increasing technification as expert knowledge obtains a significant position to develop governance. However, contrary to

[662] EC/HREUFASP (2013),6.

the Copenhagen School perspective, the use of experts is not purely related to specific technical knowledge.[663] I maintain that it is crucial to include actors from the CI, CII and ICT industry in exchanging knowledge on technical, and management levels, as well as pooling resources and capabilities with the public sector and other relevant actors. In cyber-security, the different parties have a shared responsibility to enhance cooperation and thereby, go beyond the mere application of the new securitization moves.

Accordingly, corporate organisations and businesses exercise contractual governance with their stakeholders (employees and clients), as well as protecting their corporate interests through different types of contractual terms and conditions (section 3.3.2, 4.8.2).[664] I do not imply that these private actors are technical experts in the traditional sense. However, it is clear that these private actors have developed knowledge about prevention, management and preparedness inside their organisation. In this context, it is evident that corporate organisations employ a broad range of software solutions to protect themselves, and to identify and investigate abnormal patterns of behaviour in their systems, which others can benefit from.[665] Different types of private security agents are already major providers in the payment-card industry, intellectual property investigation, and software-security, and this will progress significantly.[666] There is also global cyber-security alliances formed, that includes police-partnerships with banks, telecommunication providers and corporations to minimise the risks in these particular fields.[667]

Information from the private sectors is crucial in order to establish security structures to manage the growing cyber-risks:

> “[P]rivate actors still lack 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”.[668]

This citation is important because it raise a valid point regarding the private sector. One problem I have identified is that the private sector needs to be more visible in a broader security structure in order to improve the cyber-security management (section 6.6).[669]

[663] Hansen and Nissenbaum (2009),1157. Garcia and Palhares (2014),275-277.
[664] Wall (2007a),188.
[665] Wall (2007a),188.
[666] Broadhurst (2006),416.
[667] Broadhurst (2006),416.
[668] EC/HREUFASP (2013),6.
[669] EC/HREUFASP (2013),6.

The private sector has a responsibility to enhance the resilience against attacks and to exchange knowledge. Improvements have been made, and the private sector involvement is increasing. For example, after the Stuxnet attack on Iran, Siemens has increased its visibility and information sharing with ICT security communities. Apple has also opened up for cooperation by participating in major conferences with other security actors.[670] I emphasise, that the value of involving both the public and the private sector is important, despite the different reasons for participation. The public and private sector can both interact with making applicable guidelines, practices and standards on at least three levels; the public level, the private level, public-private level in cooperation (section 4.8.2).[671]

5.6 Oversight, Transparency and Accountability in Cyber-security Governance

Contemporary political and scholarly discourse often uses accountability as a conceptual umbrella that covers a number of other concepts, such as transparency, equity, democracy, efficiency, responsiveness, responsibility and integrity.[672] I understand that cyber-security governance is a very difficult area to oversee because of fragmented and differentiated structure (section 4.8.3). However, I believe that the agencies do decrease the transparency because they fail to publish data regarding their structure, objectives and cooperative parties. The risk distribution through these networks, nodes and agencies, create a significant tension for a number of reasons. Evidently, not all data can be subjected to public scrutiny as this would jeopardise the whole security architecture, and as a part of a wider national securitization, many of these organisations operate in secrecy with limited public accountability.[673] However, general information about the nodes, participants, aims, scope and findings could be made public, in a way, which does not compromise sensitive information. More openness and accountability would have a positive influence on the public opinion of security actors, which has been severely damaged by the Snowden revelations in 2013.

[670] Schmidt (2014),187.

[671] Scott (2002) 'Private regulation of the public sector',69.

[672] Bovens (2007), 449. Mulgan (2000), Mulgan (2003) *Holding Power to Account.*

[673] Deibert and Rohozinski (2010b),19. MacAskill et al. (2013) *"In the UK, GCHQ oversight comes from parliament's Intelligence and Security Committee, which is chaired by Sir Malcom Rifkind, who said it was part of his role to "defend" the UK's intelligence agencies. In public statements, GCHQ says it works within "the strongest systems of checks and balances for secret intelligence anywhere in the world". Internal legal briefings, however, acknowledge the agency has "a light oversight regime compared with the US", adding that the parliamentary committee responsible for GCHQ has "always been exceptionally good at understanding the need to keep our work secret".* The Guardian (2014b) 'The issues, the oversight'.

The European cyber-security approach includes networked nodes and joint ventures towards common goals. Nonetheless, there is a side-effect of the missing accountability and oversight mechanisms in the different initiatives. The Paris School are concerned about the distribution of powers internally in the nodes, and the ability to extend their power beyond the original mandate for cooperation (section 4.6). According to Bigo et al, exceptional politics do not require new political measures to deal with extraordinary security problems, but the initiatives do not address this paramount security issue. The nodal governance structure is tied to numerous security experts working within a defined area. The problem with this approach is that the structure of exceptional security practices derives from the ongoing processes of technocratic, bureaucratic, market-driven routines, and normalisation (section 4.6.4).[674] In this sense, it is problematic that these governance forms are developed internally at the nodes, because they are usually kept there without being brought forward to public knowledge. However, there are democratic check-and-balancing systems in place, but they seem a nullity if no one knows that the security actors act outside their legal foundation. This creates an intellectual and political challenge to understand and address the lack of accountability.

Accountability is not only about legal control, it also includes political, administrative, professional, and social forms of accountability, which adds to the complexity by including a number of actors, policies and checks and balances in the framework.[675] Private regulation is equally as important as governmental regulation, because it reaches another audience. Together, these regulatory forms create the multi-levelled governance, which embrace transnational and cross-sectored cooperation. Accountability and oversight mechanisms are not visible in this context due to the secret nature of the work, and because most of these private security actors are constituted as multinational or transnational joint ventures. Therefore, they are not subjected to public scrutiny in the same way as the public sector.[676] The emergence of transnational private governance constitutes a challenge to the traditional constitutional structure, substantially rooted in electoral politics and the ambition to control governmental and legislative powers (section 3.3.2).[677]

[674] C.A.S.E. Collective (2006),466.

[675] Bovens (2007),455-457.

[676] Deibert and Rohozinski (2010b),20.

[677] Murkans (2009) ‘The quest for constitutionalism in the UK public law discourses’,427-455. Scott et al (2011) ‘The conceptual and constitutional challenge of transnational private regulation’,5.

Cooperation is beneficial to security actors in order to develop and improve a security structure to manage cyber-risks. However, I believe that there is an adverse side-effect of creating these large-scale systems. This is linked to the creation of very complex and imprecise formations, where the differentiated and fragmented approach blurs the overview of activities and actors. This has also concerned the Paris School, because these actors develop exceptional measures within the nodes through their internal power struggle. It is problematic that information is not communicated to the public regarding the participants, their role and the purpose of the node (section 3.3). I find it incredibly difficult to get an overview of the networks. Europol, for example, only identifies the principle partners in general terms, and the content of their cooperation is very vaguely described.[678] I have discovered that the lack of information about participants is also significant in relation to the various EU communications, which vaguely identify the type of actors that can be involved. NATO also recognises partnership and cooperation, but the alliance is even more imprecise when discussing the different cooperative nodes.[679] After attempting to investigate this topic, and after reviewing various websites, it is evident that security actors are not explicitly named beyond the most well-known security institutions and agencies, industries and associations. As a result, I have only been able to get partial information about the security nodes and their progress, and this is a significant transparency problem.

5.7 Anticipatory Governance and the Development of Rules, Practices and Processes

To create functional governance forms in this fragmented area, it requires the use of multi-levelled regulation to cover the different cyber-risks. The nature of regulation within the national state undergoes significant changes, where flexible governance overtakes the traditional command-and-control approach.[680] A fragmented possession of resources is an essential element in the pluralistic re-conceptualisation of the regulatory processes included in nodal governance.[681] Regulatory spaces draw attention to the many forms of cooperation and the use of different agents, who have the potential to engage in the public policy-making processes (sections 3.3, 3.7, 4.8).[682] In this differentiated security environment, decentralised rules, practices and procedures become essential in mirroring cyber-risks, which can take numerous forms and

[678] Europol (2013b) ‘EU agencies’. Europol (2013c) ‘External partners’.
[679] NATO (2013).
[680] Brownswood (2008) ‘So what does the world need now?’,24.
[681] Scott (2001) ‘Analysing regulatory space’,333.
[682] Scott (2001),334.

directions. This stance originates from the character of these systems, because no one can promote their viewpoint as the only one, and by so doing bind other systems.[683] Moreover, I need to draw the reader back to the ongoing security circle presented and illustrated in chapter 3. Cyber governance is about, not only different actors, but also management forms that include different anticipatory steps. These combine anticipatory risk-management with threat-assessment. In this circle, the circular steps span from risk to threat, the condition of possibilities to securitization and from resilience to preparedness (figure 6).

Anticipatory governance and practices in itself can introduce problems if it is not carefully monitored. The different forms of preventive and precautionary measures can violate the liberty of the user through filtering undesirable contents, intimidation and self-censorship through constant surveillance, as well by disabling or disconnecting ICTs.[684] This puts limitations on governmental rules, technical regulations, and self-regulatory practices and processes, which realistically can be imposed. Cyber-security governance has to be balanced against the nature of cyber-space as an open communication platform and the rights and liberties of the users. The joint EU Communication (2013) highlights how important it is to ensure an open, free and secure Internet in order to prevent censorship and uphold human rights and fundamental freedoms. Explicitly mentioned in the security strategy is the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights, which all should be respected in online management.[685]

I have identified various procedures, which are involved in managing socio-technological cyber-risks (section 4.8). Regulation through law has a high position on the security agenda.[686] It is true that it is important for cooperation to harmonise judiciary and law enforcement measures among states in an international, regional, national context. However, I believe that this only has relevance in combination with other regulatory forms, because regulation through law only covers a limited scope, and there is severe bureaucracy problems linked to the schedule for adopting legislation. Technical regulation is another form of management that is brought into action to map the problems and develop technical solutions to the problems. Directly linked to these

[683] Smismans (2005) ‘Reflexive law in support of directly deliberative polyarchy’,2.
[684] Deibert and Rohozinski (2010b),17.
[685] EC/HREUFASP (2013),2, 15.
[686] Deibert and Rohozinski (2010b),17.

two areas are education and awareness-raising, which are crucial to enhancing protection and preparedness in the public sphere. Yet, this significant area is often overlooked, which is striking, because it has a long-term potential to change the behaviour of hi-tech users and secure their online activities. To promote self-governance, it is important to establish and promote self-defence and self-regulation, because these add another dimension to the anticipatory risk-security framework.

5.7.1 State Regulation

This discussion on state regulation follows on from the previous discussions on transnational governance. The discussion in this section will focus on the lack of harmonisation in state regulatory measures and their slow progress. The regulation of cyber-space is a security challenge which national states are unable to carry out alone (section 2.4, 3.3). In pluralist societies, the legitimacy is being challenged, as regulatory zones move beyond the national state to cover regional and international cooperation.[687] Harmonising legislation in large formations is a priority to counter all unlawful activities in/from cyber-space. Yet, we need to involve other regulatory structures and means to broaden up the scope of the anticipatory framework, because it is impossible to predict future directions of cyber-risks. The regulatory space of the virtual world operates parallel to the ordinary sphere. A country can securitize a particular area and impose emergency measures to deal with the risk, yet it is harder to get legitimacy to securitize worldwide in such a complex area. Securitization of the Internet/social media can backfire, as we have seen in Turkey's Twitter case (2014). Restrictions on internet access imposed by the Turkish government caused violent demonstrations in Istanbul, because free access to the internet is now regarded as an important part of people's personal freedom and liberty, which should not be limited.[688] Nevertheless, it is noteworthy that the ban prompted a high degree of civil disobedience, where internet users quickly found ways to get access to Twitter despite the restrictions.[689]

Regulation through law is nearly impossible to implement in a global context. Yet, guidelines and recommendations can be developed to ensure better harmonisation in the absence of an international treaty – and this has been widely used to fill out regulatory gaps (chapter 4).[690] A constant challenge for law enforcement is the difficulty of

[687] Brownswood (2008),24.

[688]The Guardian (2014c) 'Turkish police crack down on internet freedom protest'. Sinclair-Webb (2014) 'Dispatches: Turkey shuts down Twitter'.

[689] Cresci (2014) 'How to get around Turkey's Twitter ban'.

[690] Podgor (2004),102.

investigating, prosecuting and punishing the offenders when an inconsistency in regulation is maintained. The problem on the operational level is based on the lack of regulatory consensus on the strategic level. The technical development is so fast that the legislators struggle to keep up with cyber criminals, who regularly challenge the public authorities by developing new ways of using cyber-space and computer systems to commit a crime.[691] Law enforcement agencies in some countries lack knowledge and adequate resources, training at the appropriate level, or lack the desire to understand cyber-risks and unlawful cyber-activities.[692] There are also problems in communication with web-hosts in an international context. This creates obstacles for evidence gathering when carrying out comprehensive investigations, in order to prosecute and punish offenders.[693]

5.7.2 Technical Regulation

Compared with state regulation, technical regulation is more challenging, and very important, because technology is used in the anticipatory governance framework. The effectiveness, of using technology, derives from different constructions. Technology can disrupt human actions in cyber-space by blocking the information flow, and by doing so, it can force individuals to renegotiate paths and goals.[694] Involving technical regulation in risk-security enhances the use of private actors, as they have the technical and scientific knowledge that state actors often lack. Technical experts have a significant role in the rethinking of securitization. However, the use of experts is limited and only linked to the speech-act. The Paris School perspective does not have these limitations, because it includes numerous actors. The Paris School takes a different approach to everyday practices, because the school focuses on the governance forms developed through collective social groupings (section 4.6.1).[695] I, therefore, see technical regulation as part of the natural progression of the nodal system, where different forms of expertise are required for the nodes. Consequently, technical computer security actors know the area better and can make risk-assessments that are more precise. In this context, the public sector sets out the guidelines, and the private security actors develop management solutions. Close cooperation between corporations and the CoE has been established. Multinational corporations, such as Microsoft and

[691] Marion (2010) ‘The Council of Europe’s Cyber Crime Treaty’,700.
[692] Marion (2010),703.
[693] Marion (2010),700.
[694] Young (2008) ‘Towards an understanding of regulation by design’,81.
[695] Radu (2014),8.

McAfee are involved in addressing the challenges in the fight against cyber-crime.[696] Microsoft has also announced that they have entered into new partnerships, i.e. Europol. This cooperation has already proven useful, where these two parties have pooled their technological knowledge and successfully disrupted the dangerous ZeroAccess botnet, which had infected up to two million computers.[697]

Yet, the use of technical regulation creates a conflict of interests. Imposing technical restrictions or randomly obtaining information online about people's behaviour can have an adverse effect, where the authorities' response is very similar to the hackers. Dissatisfaction with authorities' actions can trigger a form of hacktivism among computer users, i.e. Turkey's Twitter ban, where the securitization was a substantial defeat for the government (chapter three). The Paris School has also highlighted instances where security professionals have used none-discriminatory routinised surveillance as a bureaucratic tool, i.e. the GCHQ scandal (section 4.6.1). The technological development has improved security actor's possibilities and opportunities to obtain information or to collect meta-data about ordinary citizens throughout the world. The increasing reliance on electronic communication suggests that more information about groups and individuals is stored in network-accessible systems. As a result, this data will be communicated more frequently and broadly, which raises the question of data security.[698] The most well-known justification for this type of information collection is to prevent terrorism and child abuse. In 2013, as part of the Edward Snowden revelations, it was discovered that GCHQ had developed sophisticated tools to manipulate online polls, spam targets with SMS messages, track people by impersonating spammers and monitor social media postings.[699]

Internet technologies present a possibility of a wider technification, where experts get to play a significant role in carrying out a speech-act along with the securitizing (section 4.5.3).[700] Intrusive policies are open to abuse if they are made to automatically filter, block or censor the internet. The Copenhagen School state-centric speech-act can be used to legitimise filtering, blocking and censoring the Internet. However, according to the Copenhagen School this can only happen when accredited technical experts are

[696] Avina (2011),284.
[697] Europol (2014b) 'Europol and Microsoft enters into new global partnerships in fight against cybercrime. Microsoft (2014) 'Microsoft enters into new global partnerships in fight against cybercrime'.
[698] Lin and Dam (1996),41.
[699] MacAskill et al (2013a). Hopkins (2013).
[700] Buzan et al (1998),36. Hansen and Nissenbaum (2009),1166. Garcia and Palhares (2014),277.

involved in the process to convince an audience of the dangers. These experts might have a more powerful voice in the public debate compared with traditional securitization actors, i.e. child-abuse images, terrorism, etc.[701] This is particularly pertinent in the current security environment, where security sectors trustworthiness has been damaged by the GCHQ and NSA scandals. Therefore, security experts can be used to circumvent the negative reputation of state actors, because the public still regard experts as trustworthy. Yet, this establishes a problematic balancing act. Experts can risk their reputation if they are caught up in the same problems as state actors. This can cause severe problems to their scientific status if they participate in developing exceptional rules and regulations internally in the nodes, and if they also begin to circumvent the limits accepted by the audience.

The focus on technical regulation entails a combination of proactive and reactive measures. This involves an extensive range of technologies developed through public-private initiatives that block, disrupt or damage unlawful activities in cyber-space. One of the problems associated with technical regulations are that they often overreact by indiscriminately blocking or filtering the content on a wider scale than intended.[702] This happens automatically, and it is often unclear what is being blocked, why, or by whom. By using technical regulation automatically, the normal mechanisms of accountability are reduced, i.e. judiciary review, media scrutiny, etc.[703] Moreover, the problem of using technological means as regulators, is to strike a balance between providing security and maintaining fundamental rights.[704] The use of technical regulation, and in particular, filtering, may result in a loss of accountability. Moreover, this raises the question of what accountability means outside the state-centric framework. For example, there is a possibility to circumvent this area by outsourcing it to private actors, such as Google and Facebook who could filter the content of their own users.

In this context, it has been positive to observe that the European Court of Justice (ECJ) recently have made significant judgements, which ensures better data protection. One famous case that involves Google establishes the EU's 'right to be forgotten',[705] and the

[701] Margretts (2009) 'The Internet and public policy',7.
[702] McIntyre and Scott (2008) 'Internet filtering',116. Yar (2006),112.
[703] McIntyre and Scott (2008),111.
[704] Wall (2007a),190-191.
[705] "*[T]he European Court of Justice ruling that makes it possible for some links to third-party content to be removed from search results through an appeals process"*. Fertik (2014) 'The 'right to be forgotten' may help protect our digital dignity' Travis and Arthur (2014) 'EU court backs 'right to be forgotten''.

second ruling restricts state access to citizens' data.[706] The ECJ ruled that current laws invade individual privacy.[707] This signifies that the new measures need to have a sunset clause inbuilt, as well as some safeguards to balance security and liberties.[708] I would argue that this accommodates my previous criticism, that the lack of oversight and accountability in both public and private context has a damaging effect on human rights and fundamental freedoms (sections 3.3.2, 4.8.3). These changes show a trend towards a more visible check on cyber-security governance forms – but it also puts pressure on decision-makers to incorporate particular control systems into security strategies, as well as national law. Nevertheless, I would argue that it is too early to state that the practice has been formed in this area. It is feasible that court oversight is adequate to ensure accountability in relation to the EU legislative framework and institutions. However, it is noteworthy that the 'right to be forgotten' is only applicable to the EU. Google cannot be forced to remove information in a global context and, therefore, the ruling has only a limited application.

These different types of technological regulation and measures call for alternative management procedures to minimise the risk of abuse. I support the argument that the use of technical regulations has given rise to concerns for individual liberty, such as the right to liberty and security, respect for private life, freedom of thought, expression, assembly and association.[709] I would argue that this creates a forum for overeager regulators to impose measures, which potentially could restrict the freedom of users.[710] Legal and technological instruments are not tools to achieve specific policy objectives. They cannot conceptualise the legal architecture of democracy and the rule of law, which safeguard interactions between citizens, the state and the civil society.[711]

5.7.3 Awareness-raising and Education

Awareness-raising and education are essential tools to decrease the vulnerability and enhance the resilience towards cyber-space attacks. This is applicable to both public-private sectors and the individual user in a private sphere. I consider this to be a very important area. Unfortunately, it has not been given the attention it requires in the anticipatory governance framework. All users are responsible for improving security of

[706] Wintour et al (2014) 'David Cameron makes concessions to rush through snooping law'
[707] Wintour (2014) 'Emergency surveillance law to be brought in with cross-party support'
[708] Paddick (2014) 'The surveillance law is a threat to criminals, not privacy'.
[709] Bowling et al. (2008) 'Crime control technologies',57.
[710] Zittrain (2008) 'Perfect enforcement',129-130.
[711] Hildebrandt. (2008),178-179.

computer systems, but the challenge of awareness is multifaceted.[712] The joint EU Communication (2013) has emphasised this problem, stating:

> "Ensuring cybersecurity is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them".[713]

However, this is not enough, because hackers have developed several ways of accessing computer systems by infecting e-mail programs or compromising computer systems, which cannot be predicted beforehand. It has been stated that:

> "[T]he ability to fool the naïve user remains one of the key tools of the hackers".[714]

Yet, it is not only the naïve, who are attacked. Technical tools, which allow unauthorised users to enter a computer unlawfully, have been enacted over the years, and this technology is still developing rapidly. This makes it difficult for an individual user to impose adequate protection, and the preventive tools available, are to some extent outdated and incompatible with new types of attack. Therefore, basic knowledge regarding protection is an integral part of the awareness-raising and education package.

Information regarding cyber-security derives from various sources. The Eurobarometer survey (2012) highlights (appendix 4):

> "The majority of EU citizens say they have seen or heard something about cybercrime in the last 12 months (73%). When shown a list of possible sources of information, respondents are most likely to say they got their information about cybercrime from television (59%). Around a quarter saw something about cybercrime in newspapers (27%) and the Internet (24%), while 19% got information from the radio and 20% from friends, family, or colleagues".[715]

This survey reveals that the mass media has played a significant role in spreading awareness of cyber-security throughout Europe. I have found that individual computer users and social media have significant experience with anticipatory governance forms and self-regulation, which is beneficial for the framework. Moreover, they create a platform for spreading information, rasing awareness and educating users. I maintain the argument that this area is a natural process to include these actors in the nodal system. These individual users are using civil society networks to inform about best practices and networking strategies, lobby governments, and operate largely irrespective

[712] Rudasill and Moyer (2004) 'Cyber-security, cyber-attack, and the development of a governmental response',253.
[713] EC/HREUFASP (2013),8.
[714] Rudasill and Moyer (2004),253.
[715] EC (2012a),35.

of national boundaries.[716] The knowledge of cyber-security needs to be communicated to a wider audience, and it is up to both public and private security actors to create a balanced level of awareness internally in the region (chapter 6).[717] The Eurobarometer survey highlights that most of the EU citizens felt that they were either not well-informed (34%) or not informed at all about cyber-crime (25%). Only 7% felt that they knew enough about cyber-crime.[718] This exposes that the information gap is prevalent in the public sphere, and this lacuna can be referred back to the communication deficit in the nodal governance structure. ENISA and some Member States have taken steps to raise awareness in a larger context. They have introduced a European cybersecurity month.[719] Whether this initiative is going to be successful is hard to tell because nobody can predict future outcome of the procedures and no impact assessment has been communicated beyond the institutions. I would argue that this pilot project has so far been very limited because it has failed to reach the target audience. Despite its lack of success, the initiative was extended and applied in the whole EU in 2013, and an EU-US cyber-security month is scheduled from 2014.[720]

The CoE Convention on Cyber-crime also has an educational and awareness-raising function on an international level.[721] It aims to inform people in all countries about safe behaviour on the Internet. Nevertheless, it fails to define what acceptable behaviour is.[722] Transnational and cross-sectoral corporations are involved in education and awareness-raising. Companies such as CISCO, Google, McAfee, Microsoft Symantec and Yahoo have engaged in several non-commercial governmental partnerships that offer Internet safety training programmes and educational literature to schools, communities and individuals. These initiatives are important for spreading knowledge and understanding about online security of individual users. Moreover, these multinational corporations provide training for public authorities on how effectively the risks nationally and transnationally can be addressed.[723] Of course, it is positive to observe that the CoE has collaborated with Microsoft to conduct training with the

[716] Deibert and Crete-Nishihata (2013),330.

[717] *There is a clear difference between the answers given in the northern/eastern part of Europe and in the southern/western part. Appendix 3.* EC (2012a),35.

[718] *There is also an unbalanced level of awareness between the countries; a significant difference between the northern or the southern part of Europe. Appendix 3.* EC (2012a),37.

[719] EC/HREUFASP (2013),8.

[720] EC/HREUFASP (2013),8.

[721] Marion (2010),706.

[722] Marion (2010),706.

[723] Avina (2011),289.

judiciary in both Egypt and Turkey. Both McAfee and Microsoft have created a joint venture with CoE for a similar training program in Romania, and it seems to be a developing trend. It has proven beneficial to involve stakeholders from the computer technology and security industries in non-commercial partnerships because they have knowledge regarding technical and practical computer problems. There are underpinning reasons for these companies to be involved. I believe that through cooperation, corporations and businesses can direct behaviour and maximise self-governance. Although they claim their involvement is non-commercial, it is impossible for the consumers to distinct the corporations' work. As a result, their role as security actors and their commercial products are blurred, and this involvement in the cooperation generally improves the branding of the corporations (chapter 4).

The CoE is not the only actor to be involved in education and awareness-raising. The EU Action Plan emphasises the necessity of guiding individual users on security in cyber-space. It obliges Member States to ensure that citizens have easy access to guidance and information concerning cyber threats in order to take basic precautions. I think that these forms of information enables people to protect their privacy online, detect and report grooming, equip their computers with the necessary security software, manage passwords and detect phishing, pharming or other attacks.[724] ENISA also include education and awareness-raising on their agenda in order to maximise preparedness towards security risks related to cyber-space. I believe that this is an active development towards a more inclusive framework that invites other actors to play a more visible role. This initiative is directed towards European citizens, and small/ medium-sized businesses who do not have the same access to adequate information as the EU institutions, the Member States or multinational-corporations.[725] The question here is how much normative influence this security agency has at the operational level, because so far they have not been successful in spreading information to the public.

5.7.4 Self-defence and Self-regulation

Self-defence and self-regulation are the outcomes of the anticipatory governance and practices developed through cooperation between securities actors. The regulation of cyber-space is seen as an external negative form of management that contradicts the rationale behind the Internet. However, there are regulatory spaces left for developing

[724] EC (2010i),10.

[725] ENISA (2013b) 'FAQ on ENISA and ENISAS,2.

standard settings, monitoring and enforcement, and not all forms of regulation are necessarily linked to governmental or technical regulation. The private sector, web-hosts and social-networks are the primary security actors in this area, which empower them to govern the conduct of their users.[726] I argue that it relevant to look at both self-defence and self-regulation as interlinked with anticipatory cyber-security on the individual level, because it functions as a supplement to the traditional governance (chapter 3). Users are advised to take the basic security precautions in line with the risks they are subjected to through usage.[727] Individuals can protect their passwords and invest in basic computer software, for instance, anti-virus, firewall, anti-spyware, identity protection, anti-rootkit and anti-spam to minimise the security risks. The public sector, private institutions, organisations and businesses also incorporate self-defence/ preventive measures into their security strategies by investing in security protection, and by educating employees about risks.

Based on the research in this thesis, I would argue that alternative forms of preventive measures arise from the users themselves. Cyber-space, as such, is not a dangerous and unruly place. The conduct of the computer users themselves provides opportunities for cyber-attacks.[728] Therefore, the users and the online community also have a responsibility to enhance resilience and preparedness through self-defence/ self-regulation. Williams states:

> "There is much to be learnt about online communities, social control, and regulation for the citizens that are integral to their creation, sustainability, and maturation. Understanding these "native" or "grassroots" processes is essential to the development of more general regulatory practice beyond individual online communities".[729]

Williams's comments highlight that government policies and behaviour are a result of the activities of different actors, such as civil society networks and the private sector that function as a conduit and communicator of ideas and policies.[730] There is a significant level of self-governance and self-defence included in this area, which cannot be overlooked (section 3.3). Yet, it seems like this dimension is largely forgotten when discussing nodal governance. It is important to learn from these everyday practices developed by individuals and online communities. I believe that this goes beyond

[726] Scott (2002),60.
[727] Grabosky (2007a), 93.
[728] Williams (2007) 'Policing and cybersociety',61.
[729] Williams (2007),61.
[730] Deibert and Crete-Nishihata (2013),330.

learning from individual experiences as promoted by the Copenhagen School. They claim that the new move is understood, in a way, where the acceptance of public security discourses may be facilitated with the concrete experiences of individuals (section 4.5.2).[731] Yet, I dismiss this argument, and state that these online communities have experienced with different techniques and have developed a set of rules that functions in practice within a limited space. Some grassroots processes can form the backbone for the general regulation beyond the online community. As these virtual environments become more established and populated, the need to maintain order increases.[732] From my perspective, these individuals are vital to the security-nodes, because these networked communities have particular expertise about the Internet, the behaviour of their users, and its regulation. Individuals and online communities are not the only actors relevant in order to impose self-regulation. Other actors influence the conduct and developing anticipatory practices to protect individuals. Companies, such as Google, Yahoo, Microsoft, Apple, etc. are all major players who can change behaviour on the Internet, and these companies are already deeply involved in different regulatory functions by regulating the conduct of their customers.

5.8 Conclusion

Following the theoretical synthesis of the risk-security literature, I would argue that cyber-security strategies are centred around the three areas discussed in chapter 4. Security actors, cooperation and anticipatory governance and practices all have an integral part in the cyber-security discussion (section 4.8). However, the analysis casts a distinctive light over particular security problems. I argue that this area is not predominate state-centric, nor entirely an open-ended form of governance. The state-centric approach still has a stranglehold in relation to transnational cooperation in the European region; yet, the traditional use of this method is in retreat. Even the Copenhagen School has accepted that other actors can replace the state-actor in the speech-act that enables exceptional responses (chapter 4). I think that the Copenhagen School's rethinking is too narrowly formed to accommodate the broad spectrum of regulatory issues and security actors, and despite its improvements, it fails to have any significant impact on the development of cyber-security governance forms. Collaborations are not formed traditionally, because there are links to transnational and private security agents. From that perspective, I emphasise that strategical security is

[731] Hansen and Nissenbaum (2009),1165. Cf. Williams (2007),61
[732] Wall (2007) 'Policing cybercrimes',188.

overwhelmingly based on the nodal governmentality approach, where states are just a node among others. In the transnational context, states still hold a strong position in transnational cooperation. On the contrary, cross-sectoral cooperation is purely open-ended and not tied to old cooperative alliances. Instead, I maintain, that this contains a different combination of actors, which creates a more innovative foundation beyond the state-centric approach. As a result, I would argue that this implies that the pure state-centric foundation is fundamentally misplaced in the cyber-security structure.

The merger between the internal-external and public-private dimensions creates obstacles. I have discovered that there are fundamental differences between the hierarchical and bureaucratic nature of European institutions and cooperation. The two different approaches struggle to embrace the structure of nodal governance, which includes states, agencies, businesses, groups and individuals. I would argue that legislation and governance forms are processing through the system in a very inflexible way characterised by its slow pace that create lacunas in the management structure. Additionally, there are significant problems with harmonising the national initiatives and implementing regulation deriving from the European institutions. In the chapter, I have highlighted and discussed different issues which have supported the Paris School's concerns about the increasingly complex and fragmented cyber-security structure. Differentiated management jeopardises fundamental principles, such as openness, transparency and accountability. I believe that the most significant problem is linked to the lack of communication, where information is kept internal in the nodes, and oversight mechanisms are left out of the strategies. We can only presume that rules will be developed within a politicised area, and therefore, they will follow a democratic check and balancing system within the national state. However, as the Snowden revelations have shown, there is clearly a problem with independent scrutiny and public information regarding security strategies.

6 Cyber-terrorism: An Emerging Security Risk

6.1 Introduction

The U.S. Secretary of defence, Leon Panetta stated in 2012, that:

> "A cyber attack perpetrated by national states or violent extremist groups can be as destructive as the terrorist attacks on 9/11".[733]

He continues,

> "Such a destructive cyber-attack could paralyse the nation".[734]

This sounds like science fiction. However, reality is becoming closer to this approach every minute, because cyber-terrorism has reached an exceptional technological level, which makes it difficult to manage. Critical infrastructure (CI), Critical information infrastructure (CII), and information computer technologies (ICTs) are considered vital parts of the daily activities of the European economy and society, i.e. sharing/developing information and communication technologies, services, networks, and infrastructures. The acknowledgment of cyber-terrorism risks began in 2007 with the three-week wave of cyber–attacks on Estonia's government, telecommunication, news organisations and banks, which caused mass disturbance internally in the country (section 3.4). As a result, the global focus on cyber-terrorism has changed significantly.[735] Before these corresponding cyber-attacks, organisations treated cyber-risks in isolation, and anticipatory plans were merely incorporated into individual contingency plans without coordination in a larger context.[736]

Therefore, I would argue that different types of anticipatory governance forms, related to counter-terrorism and cyber-crime legislation, cover cyber-risks. Cyber-crime and counter-terrorism measures are specific for this area because there is an overlap between them which make this area a particular problem in the anticipatory cyber-security framework. This requires special attention, and I have separated the two concepts in the definition. I have centred the discussion in this chapter on cyber-terrorism, as well as the development of management structures to enhance resilience and preparedness against these security risks. This study supports the arguments in the previous chapter, where cyber-security was discussed from a broad perspective. Similar to the first case

[733] Ratnam (2012) 'Cyber attacks could become as destructive as 9/11: Panetta.

[734] Ratnam (2012).

[735] Tikk (2011),119. The Guardian (2007) 'Russia accused of unleashing cyberwar to disable Estonia'. Hansen and Nissenbaum (2009),1168. Radu (2014),12. Schmidt (2014),190.

[736] Tikk (2011),119.

study, the analytical framework is based on nodal governance and the development of anticipatory governance and practices. This supports the research objectives from chapter 1, where I aim to generate insight into an emerging security concern. Firstly, I will examine cyber-terrorism and cyber-attacks from a general perspective. Secondly, I will discuss cooperation, e.g. transnational and cross-sectoral cooperation. In this part, my primary focus is on cross-sectoral, i.e. public-private partnerships (PPPs) and their relevance to security governance, because this is a significant area of cyber-terrorism where both public and private actors can be at risk. Thirdly, I will investigate the development of anticipatory governance forms necessary to enhance security on multiple levels.

6.2 Defining Cyber-terrorism

In support of my claim that this area requires a separate analysis beyond the overarching cyber-security governance structure, I focus on the definitional problem that traps cyber-terrorism between cyber-crime and the traditional terrorism regulatory framework. The legislative complexity makes this a significant area to discuss. As this particular risk is a sub-category of the cyber-security framework, it is possible to go more in-depth regarding particular areas of the framework, which is not adequately defined and established. In this context, Europol has correctly claimed that there are definitional problems regarding the term cyber-terrorism:

> “There is a lack of international consensus concerning the term “cyberterrorism”, which is used variously to describe activities including electronic attacks on critical infrastructure, intellectual property theft relating to research and development, and even the use of Internet technology for the dissemination of propaganda or for communication purposes”.[737]

The inclusivity of these different areas depends on the interpretation of the attack and the motivation of the hackers. According to Interpol, the threat of terrorism, for example, forces authorities to assess and develop action plans to protect particular security vulnerabilities:

> “[T]he threat of terrorism forces authorities to address security vulnerabilities related to information technology infrastructure such as power plants, electrical grinds, information systems and the computer systems of government and major companies”.[738]

[737] Europol (2011b),11.

[738] Interpol (2013) ‘Cybercrime’.

Cyber-terrorism merges two significant security risks, namely, terrorism and cyber-crime. The main difference between these two is the platform used to attack.[739] Cyber-terrorism uses a virtual world as a measure to spread fear, damage, and communicate (section 2.6.3). Whereas, terrorism has traditionally been distinct from routine criminal violence, and is mainly considered an extreme form of violence executed for political, ideological, or religious reasons.[740] The difference between the two concepts relates to terrorism, which entails a more direct threat of violence compared with cyber-terrorism. A cyber-attack might not trigger a large number of causalities. Nevertheless, cyber-attacks have an enormous potential to create catastrophic events, such as shutting down a large portion of power plants. Cyber-attacks on major facilities such as power plants have a similar effect, if not greater, than taking down an airplane.[741] If we consider using worst-case scenario/hyper-securitization to image future cyber-risks, a likely scenario could be cyber-attacks that prompt satellites to spin out of control, overtake control of airplanes, power plants to break down, economies to crash or groups and individuals being deprived of essential services.[742] After the attack on Estonia in 2007, the speaker of the Parliament, Ene Ergma, said:

> “When I look at a nuclear explosion and the explosion that happened in our country in May, I see the same thing”.[743]

Cyber-terrorism can be defined by combining the definition of terrorism with the use of cyber-space. Embar-Seddon defines this area as:

> “Cyber-terrorism is a form of terrorism, which uses cyber-space to spread fear and/ or damage in order to attain political, societal or economic goals using computer technology”.[744]

Despite the weakness of this definition, I would argue that it covers what is left out of the traditional terrorism definition. Arguably, it is part of the same logic, but the weapons used to attacks are different, and this needs to be incorporated to cover the differences between the virtual world and reality. In fact, it is impossible to pin down a clear and sustainable definition. One way in which cyber-terrorism is defined is:

[739] Embar-Seddon (2002) ‘Cyberterrorism: Are we under siege?’,1035.

[740] UN (2004c) ‘Security Resolution 1566’. Wilkinson (2011),5. Mythen and Walklate (2006). 391. Rehn (2003) ‘Excessive reliance on the use of force does not stop terrorism’.
Hoeksema and Ter Laak, *Human rights and terrorism*, 55. Wilson (2003) ‘Bibliographical essay on fear’,119.

[741] Embar-Seddon (2002),1038.

[742] Shackelford (2014) ‘Managing cyber attacks in international law, business, and relations’,XIX.

[743] Poulsen (2007) ‘“Cyber-war” and Estonia’s panic attack’. Dunn Cavelty (2013),117.

[744] Embar-Seddon (2002),1036.

> "[T]he intentional use of threat of use, without legally recognised authority, of violence, disruption, or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm".[745]

Cyber-terrorism is also interpreted as a premeditated, politically motivated attack against information, computer systems, computer programs and data. Denning argued in 2000:

> "Cyber-terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injuries, explosions plane crashes, water contamination, or severe economic loss would be examples".[746]

This attack form results in violence against non-combatant targets by sub-national groups or clandestine agents.[747] Times have changed, and cyber-terrorism is not only linked to attacks against states, but also attacks against civilian populations. Denning, however, does not agree with this point, arguing that serious attacks against CI's could be an act of cyber-terrorism, but it would depend on its impact. Therefore, attacks, which disrupt non-essential services or those that are only an expensive nuisance, would not be considered as cyber-terrorism.[748]

6.2.1 Critique of Denning's Narrow Definition of Cyber-terrorism

Denning's lack of recognition of the private sector, as a possible target for terrorism, does not go unnoticed. Therefore, I consider her definition too vague and inconsistent with the reality of targeting public and private sectors, groups and individuals, and the nature of cyber-security (chapter 2 and 5). Non-essential services are problematic to define. They might be non-essential for the population as a whole, but not for the owner or provider of the service. Therefore, it is important to look at the motivation behind the attack. If the attack falls under the scope of cyber-terrorism, it does not matter if it is directed towards non-essential services, because it will still have an impact, no matter what. The attack can also be directed to expensive targets or targets of cultural significance, which does not directly influence everyday life in the same way as attacks

[745] Jones (2005) 'Cyber Terrorism',4.
[746] Denning (2000),1. Gordon and Ford (2002) 'Cyberterrorism?',637.
[747] Pollitt (1998) 'Cyberterrorism: Fact or Fancy',8. Embar-Seddon (2002),1036.
[748] Denning (2000),1. Gordon and Ford (2002),637.

against CI or CII. However, in my opinion, this will still be classified as a terrorist attack. Moreover, if the target is valuable, the attack will be profiled in the mass media, and thereby, the terrorist organization has obtained one of their objectives.

The perception of cyber-terrorism has changed, and I consider Denning's definition inadequate to cover the scope of cyber-terrorism. The joint EU Communication (2013) highlights that:

> "Cyber-security incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins - including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes".[749]

This document, for example, draws attention to the rapid development of cyber-security and the possible attacks, intentional and unintentional, against various targets, where the only limitations are linked to the imagination of the terrorists and their technological ability to launch an attack. This highlights the need for resilience and preparedness in order to maximise security. The ability to resist attacks covers three areas: cooperation of operational and policy aspects of the governmental organisation, harmonisation through international cooperation and legal frameworks, and the involvement of non-state security actors (chapters 2 and 3).[750]

The CoE states that the 'goods' of the Internet, such as ease of access, lack of regulation, vast potential audiences, and the fast flow of information, can be turned into 'bads'. These 'goods' gives advantage to terrorist groups, which are committed to terrorising societies to achieve their goals (chapter 3). These groups can be the same as those using conventional terrorist methods, i.e. same groups, new methods (IS, Al Qaeda) – or they can be new groups entirely, who use computer technologies to archive their goals (Group Anonymous). CODEXTER (CoE) has suggested that cyber-terrorism and the use of the Internet for terrorist purposes comprise several elements.[751] Firstly, cyber-attacks through the Internet can cause damage to not only essential electronic communication systems and IT infrastructure; they can also damage other infrastructure, systems and interest areas (appendix 6). Secondly, distribution of illegal material, which involves propaganda, fundraising for, and financing of terrorist

[749] EC/HREUFASP (2013),3.
[750] Klimburg (2011),43.
[751] CODEXTER (2007) 'Opinion of the committee of experts on terrorism.

activities, training and the recruitment of terrorists. Thirdly, the term cyber-terrorism also includes other logistic use of IT systems by terrorists, which covers internal communication, information acquisitions and target analysis. As a result, the term includes a larger group of targets in relation to damage CI, CII and ICTs.

Targeting the private sector or individuals is not a new idea. Traditional terrorism has used private targets as a mean to an end, i.e. the Al-Qaeda attacks on the Twin Towers in New York and Pentagon in Washington DC (2001), the Madrid train attacks (2004), the attacks in London (2005), the IRA attack on Arndale Centre in Manchester (1996). The list is endless. For decades, these attacks have been done to create a climate of fear through actions with the purpose

> "[T]o destroy or undermine democratic governments and to impose their own agenda by coercive intimidation".[752]

Using CI, CII and ICTs, to carry out attacks – or to target these services - have severely affected owners and providers, as well as their customers. However, there is a shift on Internet hacktivism and terrorism attacks, because the motivation for attacks does not necessarily have to be linked to the public sector, the government or the establishment. Hacktivism towards particular private companies can be imposed because of a specific business case, cooperation with other companies, cooperation with states, and/or because of the companies' general behaviour (local, national, regional and international). Targeting private corporations is significantly visible in the Group Anonymous' attacks.[753] The same with the Stuxnet attack against Siemens equipment, where the code was written to attack material from this particular provider.[754] Another high-profile virus attack in 2012, Shamoon, wiped out the hard drives of tens of thousands of Saudi Aramco computers, and left a picture of a burning American flag on the screens of the attacked devices.[755] However, due to the lack of legislative measures, attacks against the private sector may fall under the scope of different national counter-terrorism, cyber-crime legislation or ordinary criminal law.

6.2.2 Increasing Number of Cyber-attacks

Despite the fact that states, organisations, groups and individuals now consider cyber-terrorism to be a growing concern, limited information has been published about cyber-

[752] Wilkinson (2011) Terrorism versus democracy,6-8, 25-26, 31-33.

[753] BBC News (2010a) 'Anonymous hacktivists say WikiLeak war will continue'. EURACTIV (2012) 'European renewable power grid rocked by cyber-attack'. Dunn Cavelty (2013),113.

[754] The Economist (2014a) 'Defending the digital frontier'. Dunn Cavelty (2013),111.

[755] *A Saudi Arabian oil and natural-gas giant.* The Economist (2014a). Clapperton (2013).

terrorism in Europe. Cyber-terrorism is usually discussed within the parameters of terrorism or cyber-crime. Yet, very little attention is given to the problem by the European Police Office (Europol)/ European Cybercrime Centre (EC3),[756] the CoE,[757] or NATO.[758] By searching through documents in EUROPA, it is possible to identify a large number of publications concerning the word cyber-terrorism. Nevertheless, I have not been able to find one single portal, which collects specific information about this topic.[759] One reason derives from the unbreakable link to terrorism, which is an area that is still largely securitized – and had been so since 'War on Terror' began (sections 2.4.1, 4.4). This means that terrorism is considered as a state concern, and the state is deemed the primary security actor on both the strategic and the operational level. There is a possibility that anticipatory governance and practice are developed outside the democratic processes, which constitutes a secret area as soon as the speech-act has been successful. However, cyber-terrorism is distinct from the traditional interpretation of terrorism by its connection to cyber-space. This combination of terrorism and cyber-crime legislation weakens the link to securitization significantly, because the attacks are based on hacktivism towards public and private actors and their activities, in and through, cyber-space.

To illustrate the nature of the problem and the increase in attacks, I have created appendix 5 to summarise some of the cyber-attacks carried out in recent years. This figure only shows a limited number of cases because some remain secret or undiscovered for different reasons, e.g. the nature of the attack, the nature of the target, or the attacks are not reported.[760] However, appendix 5 (figure 8) is developed using available online data mostly from mass media. I have simplified the findings in the graph below.

[756] *It is possible to find a limited number of publications using the search word 'cyber-crime terrorism'* Europol (2014a) 'About Us'.
[757] *It is possible to find a web-page and a database searching for terrorism*. CoE (2014a) 'Action for Terrorism'.
[758] *12 entries are found using cyber-terrorism as search word. However, it is to some extend justified as NATO is a military alliance, so the terrorism covers only a limited part of the scope*. NATO (2014) 'Search'
[759] EU (2014) 'Search'
[760] Yar (2006),12-15. Wall (2007a),17-20.

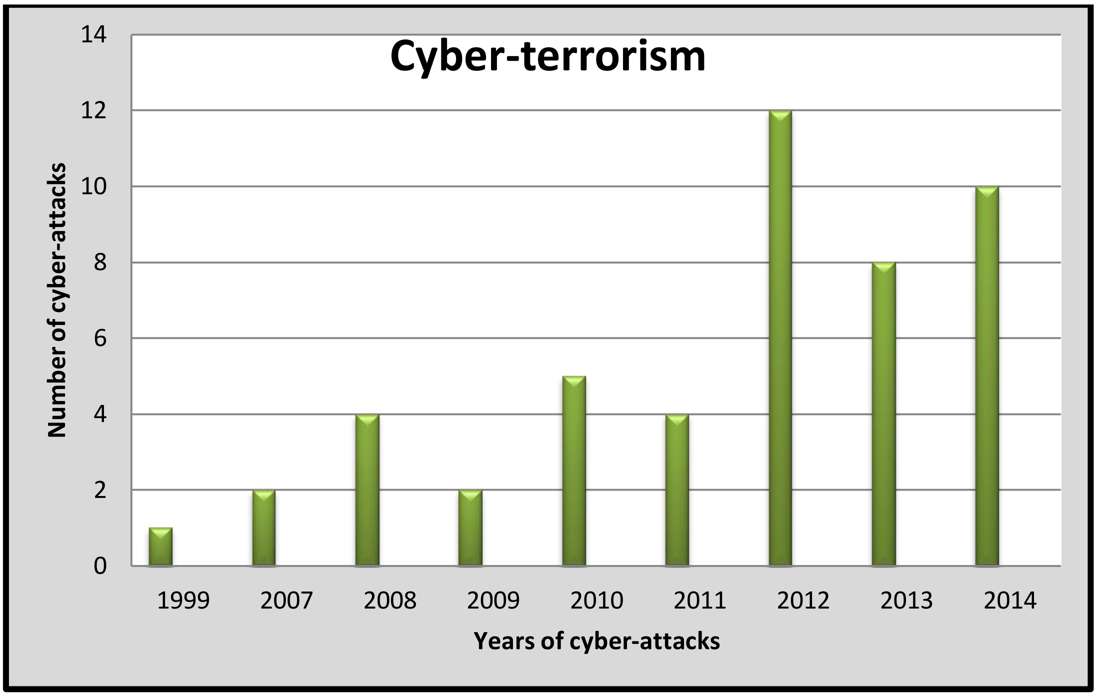


Figure 8 cyber-attacks (1999–2014) based on appendix 3

In total, I have discovered 48 large-scale cyber-terrorism cases. In appendix 5 (figure 8), I have only focused on attacks that have disrupted or destructed computer systems, as this characterises cyber-crime. There are two areas in the grey zone between cyber-terrorism, cyber-crime and cyber-warfare/information-warfare, which circumstantially can fall under the scope of cyber-terrorism. It is possible to conclude two things: Firstly, the attacks have become more sophisticated. Secondly, the number of cyber-attacks is rising, with significant peaks in 2008, 2010 and 2012. This is not a comprehensive overview of attacks, because campaigns launched by Group Anonymous, for example, have continued over several years, i.e. Project Chanology/Operation Pay-back (appendix 5). There are also examples of other ongoing campaigns between a country and a private organisation/corporation (China vs. Google). Other examples can be state-to-state disputes (the U.S. vs. Iran/ South Korea, the U.S. vs. North Korea vs. South Korea, China vs. the U.S.). In 2012, the Group Anonymous was very active; however, it slowed down its activities after that. Yet, the number of attacks has doubled if we compare 2011 (4 attacks) with 2013 and 2014 (8 attacks each year). It is significant, that the minority of these large-scale attacks are carried out in Europe. Yet, I have no data concerning the impact of the European cyber-security governance, so this observation is not evidenced with reliable data.

6.3 The International Dimension

It is not possible to ignore the international dimension concerning cyber-terrorism, because the nature of this offence creates an extraordinary need for concerted actions from an extensive source of security actors due to the extra-territorial nature of the attacks. The EU Internal Security Strategy stresses the importance of international cooperation, as internal security cannot be achieved in isolation from the rest of the world. To develop a comprehensive cyber-security framework, it is essential to create consensus between the internal and the external aspects of EU security. The strategy recognises that the relationship with partners, in particular, the U.S, is necessary to counter serious and organised crime, and terrorism.[761] This supports the Paris School's argument that the boundaries between external and internal cooperation becomes blurred and this influence the transparency and accountability. Accordingly, the internal-external nexus influences the policing of the area in a transnational and cross-sectoral context, and it is evident that the activities are significantly complicated (section 4.6.3).

Following on from the discussion in the previous chapter, there are a number of international institutions involved in developing counter-measures and governance forms. It is an important weakness in the anticipatory framework that there has not been the development of any particular cyber-terrorism treaty and legislative framework. Therefore, the CoE's Cyber-crime and Terrorism Conventions[762] the UN Conventions on Terrorism[763] and it the UN Convention against Transnational Organized Crime are the only international treaties to cover the growing risks of cyber-terrorism (chapter 5).[764] The EU strategic security framework is outlined in the Stockholm Programme, and this includes both terrorism and cyber-crime. However, within the EU security framework, numerous terrorism and cyber-crime legislations and non-legislative measures have been developed (appendix 8). The combination of regulations creates a significant challenge to understand the division between these legislative frameworks. Cyber-terrorism, as a risk to society, is widely recognised. However, developing specific regulation takes time, because it follows the slow processes discussed in the previous chapter. It is, therefore, important to develop a range of anticipatory governance forms and practices to fill the vacuum. The problem here is not outdated legislation, but the lack of explicit formulated cyber-terrorism legislation.

[761] EC (2010f),3.

[762] *The Lisbon Treaty now allows for EU's accession to the Council of Europe – it is currently being discussed at Council level.*

[763] UN (1994). UN (2004c) 'Threats to international peace and security caused by terrorist acts'

[764] McCusker (2006),259. UN (2004b).

6.4 Cyber-terrorism Cooperation

Following on from the discussions in the previous chapters, nodal cooperation is central to counter cyber-terrorism. I have analysed this topic through the lenses of nodal and anticipatory governance, which is the preferred security foundation to increase resilience and preparedness against attacks (section 3.7.1). Chapter 5 has set out the regulatory framework for discussing the different initiatives developed to manage all types of cyber-risks, whereas this chapter becomes more specific in analysing particular cyber-terrorism issues. I have chosen to investigate the regulatory framework imposed to manage a cyber-terrorism. This is done despite the fact that is not fully developed, because regulators have been reluctant to define and react to the specific nature of cyber-terrorism risks. They have considered cyber-terrorism to fall under the scope of anti-terrorism legislation. Yet, I claim that there are significant differences between an attack on a physical location, and an attack carried out in/from a virtual space, where the traditional rules and regulations are not applicable. As a result, the arguments and critique of the governance forms used in the previous chapter on cyber-security are also applicable to the cyber-terrorism analysis. My arguments concerning the lack of harmonisation, accountability, oversight, and transparency can be transferred directly to this chapter. To avoid direct repetition of arguments, I have chosen to narrow down the study of cooperation by focusing mostly on cross-sectoral cooperation. This underdeveloped area is being reconstructed in the current security strategies to mirror the risks and the growing recognition of the cyber-terrorism.

The national state can exercise effective management of CI, CII and ICTs located in the territory, i.e. ensure availability and quality of logs, develop a reporting system and create an overview of the providers - and to assess the risks and the capabilities existing within the jurisdiction.[765] It is significant that a part of this area is still securitized due to the ‘War on Terror’, and the idea that only the state can protect the population. Cyber-terrorism cooperation has generated a strong political-military approach where the state has the superior role of maintaining civil peace, territorial integrity and governmental functions to manage the challenges arising from its citizens.[766] This has resulted in cyber-security measures, which are deeply rooted in the political relations, combining military and political sectors. These two sectors have an impact on society and the

[765] Tikk (2011),121.

[766] Buzan et al (1998),50. Hansen and Nissenbaum (2009),1161.

economy due to societal dependency on electronic communication systems.[767] Securitizing a problem is primarily a political act, which has the overall purpose of protecting the sovereignty of the state which is being attacked.[768] The rhetoric used in this area is similar to the one used in cyber-warfare. Cyber-warfare faces similar legislative problems as cyber-terrorism, because they both are captured in two areas, i.e. terrorism and cyber-crime, and conventional warfare and cyber-crime. This creates an unbalanced relationship between the two types of legislations because cyber-crime merely covers economic and social complications which are remote from direct attacks in order to damage CI and/or CII. The militarisation and politicisation of terrorism creates a stronger state-centric approach compared with cyber-crime, and this gives the state a central position in deciding which areas should be securitized. Nevertheless, the securitization is inadequate to cover the private dimension. This is a significant area, where the state-centric dominance weakens and gives space to nodal governance and multi-levelled cooperation (section 4.4).

The governance structure can be linked to the reinvention of securitization (section 4.5). As a result, it is possible to understand the rationale behind extending Copenhagen School's framework, because state actors and security experts have a significant position. Yet, the role of technical experts goes beyond the characterisation of the Nissenbaum and Hansen's new security approach.[769] Computer experts are not only given the technical role, but they are also a part of actively communicating technical rhetoric to an audience.[770] The Paris School expresses a concern about the use of securitization, because it emphasises the politicisation of a problem and the mobilisation of groups and technologies. This is an area which enables security actors to create a certain truth between the link of terrorism and cyber-space (section 4.6). This interpretation of the security problem and the following speech-act imposes further implications to the sub-categories that are dragged into the securitization, i.e. surveillance, border control, CI, CII and ICTs.[771] Individuals have a less visible position in the public debate, but they can be used to provide background information about possible attacks.[772] Although, every-day routine-like processes lack the intensity of an exceptional decision, it cannot be dismissed as being without real meaning for an

[767] Buzan et al (1998),52. Kassah (2014),67.
[768] Buzan et al (1998),141.
[769] Hansen and Nissenbaum (2009),1166. Garcia and Palhares (2014),277.
[770] Hansen and Nissenbaum (2009),1167. Huysmans (2006), 6-9. Garcia and Palhares (2014),276-277.
[771] Bigo (2002),65.
[772]Hansen and Nissenbaum (2009),1165. Garcia and Palhares (2014),276.

understanding cyber-security.[773] The individualisation of cyber-security cannot be left out of the framework, because self-governance is at the forefront for preventing individuals being attacked, or involuntarily being involved through secret computer take-overs (botnet).

The two approached involved, i.e. counter-terrorism and cyber-crime creates tension in the governance structure. These tensions are linked to the fact that counter-terrorism measures are mostly state-centric, and cyber-security involves multiple security actors. However, cyber-terrorism is not only a state concern, and therefore, it cannot be articulated as a state discourse. The nature of CI, CII and ICTs circumvent this by using multi-levelled governance forms, which deepen the security agenda (section 4.3). The interconnectivity of cyber-space makes it difficult to manage the area alone without reaching out for other collaborators, i.e. transnational and cross-disciplinary cooperation between legal, policy, and military providers and operators and technical experts, businesses, groups and individuals to maximise resilience.[774] This enlarges the reinvention of the securitization approach, which only included a limited field of computer experts.[775] Cyber-security can only advance through knowledge-exchange about risks, computer technologies and management forms. As a result, I would argue that it is possible to create anticipatory governance by including a range of security actors (section 3.7).

6.5 Transnational Cooperation

The discussion in the previous chapter was concerned with the need for transnational cooperation, and highlighted the lack of international treaties, and the problems of harmonising measures and operations. These arguments are also valid in this chapter, and therefore, I will not repeat these arguments. However, there is a large incitement to protect CI, CII and ICTs, as they constitute the backbone for all computer-traffic in the modern technology-based society. Therefore, tools are developed in terms of protection against possible attacks rather than develop measures that explicitly cover cyber-terrorism. The EU encourages Member States to cooperate globally to increase the protection. Cooperation with countries and international organisations has a significant place in the EU Digital Agenda.[776] The EU Communication (2011) stresses that:

[773] Cf. Bigo (2002). Bigo (2001) ‘The möbius ribbon of internal and external security(ies)’. Van Munster (2005),6.
[774] Tikk (2011),123.
[775] Hansen and Nissenbaum (2009),1167. Garcia and Palhares (2014),277.
[776] EC (2010b).

> “We need to promote a global culture of risk management. The focus should be on promoting coordinated actions to prevent, detect, mitigate and react to all kinds of disruptions, whether manufactured or natural, as well as to prosecute related cyber-crimes. This includes conducting targeted actions against security threats and computer-based crime”.[777]

This stance has also obtained a prominent position in the 2013 joint EU Communication.[778]

6.5.1 The EU and External Cooperation

The EU’s external security policy is set to cooperate through bilateral and multilateral agreements. This increases the use of global collaboration with other countries and the agencies to minimise the risk of cyber-terrorism through the harmonisation of legislative and judiciary powers. Conversely, it is important to establish a dialogue based on mutual interests, concerns and possibilities.[779] In the EU Internal Security Strategy, transnational cooperation is explicitly mentioned:

> “Internal security cannot be achieved in isolation from the rest of the world, and, therefore, it is important to ensure coherence and complementarity between the internal and external aspects of EU security […] As that strategy recognizes a relationship with our partners, in particular the United States, are of fundamental importance in the fight against serious and organised crime and terrorism”.[780]

The lack of international consensus in regulating cyber-terrorism calls for a closer cooperation to develop good practices and processes compatible with national law, and in particular, securitized areas related to terrorism, to avoid conflicting measures. The differentiated management structures and the lack of harmonisation of law enforcement and judiciary mechanisms globally, leave cyber-space open to cyber-terrorism. CIIP is not only about anticipatory governance and strategies, but it also involves a deeper understanding of the needs of the technical community to develop workable proactive security measures. However, the lack of sustainable cooperation structures creates a fragmented and inefficient management structure globally.[781] The executive director of ENISA, Helmbrecht, supports this argument by highlighting the need for a truly international, global approach to cyber-security, which cannot be obtained in isolation:[782]

[777] EC (2011a),7.
[778] EC/HREUFASP (2013).
[779] EC (2010f),29.
[780] EC (2010f),3.
[781] EC (2009b),2.
[782] Continuity Central (2011) ‘Cooperative models for effective public private partnership’.

> “There is a need for a truly international, global approach to cyber security and critical information infrastructure protection. No country can create a CIIP strategy in isolation, as there are no national boundaries in cyber-space. PPPs are consequently one of the agenda items for the special EU-US Working Group on cyber-security and cyber-crime”.[783]

The establishment of the EU institutions, EUROPOL and the European Union’s Judicial Cooperation Unit (EUROJUST), improve the level of law harmonisation and, thus, give fewer opportunities for transnational cyber-terrorists to make use of regional loopholes.[784] As outlined in the previous chapter, there are countries that do not recognise the problem, or they have a different interpretation of cyber-risks. This creates significant obstacles to further the development of anticipatory governance forms. These problems are not only related to transnational cooperation on the strategic level; the same barriers are visible on the operational level. For instance, Russia refused to cooperate in the Estonia-case (2007) to investigate the cyber-attack.[785] The same happened in the Lithuania-case (2008),[786] and the Georgia-case (2008).[787] This is also the situation with China, which denies all involvement in cyber-attacks (appendix 5). Both Russia and China block international cooperation and the development of treaties, and this creates a significant setback for developing cyber-terrorism measures.

EU security agencies reach out to other security actors, because it is important to establish a wider nodal network with transnational collaborators outside the region. This requires that different participants are involved and have explicit knowledge about areas such as, cyber-security, anticipatory governance, cyber-crime and counter-terrorism measures. EC3 has significance in relation to internal management, and it also acts outside the realm of the EU, i.e. non-EU Member States, and the Interpol’s Global Complex for Innovation (Singapore).[788] Transnational cooperation aiming to develop sound practices and guidelines are the first step forward to increase the critical information infrastructure protection (CIIP). The EU is already engaged closely with the US on cyber-security and cyber-crime. Cooperation with the U.S. is established, and progress is made to develop networked PPPs based on strategic dialogues and

[783] Continuity Central (2011).
[784]Broadhurst (2006),422.
[785]Tikk et al (2010) ’International cyber incidents’,27. Hansen and Nissenbaum (2009),1170.
[786]Tikk et al (2010),51-53.
[787]Tikk et al (2010),89.
[788] *EC3’s collaborative partners are EU Member States; key EU stakeholders; non-EU countries; international organisations; internet governance bodies and service providers; companies involved in internet security and the financial sector; academic experts; civil society organisations; National Computer Emergency Response Teams (CERTs) and the CERT-EU.* EC3 (2014b) ’Joining forces to catch the criminals’. EC (2013a) ‘Action 32’.

cooperation external to the EU and international organisations. Knowledge of computer technology is crucial, and it is a fact that a significant part of the hardware/software industry is placed outside the European region. As a result, it is crucial to reach out to other actors.[789] Although the U.S. is a significant partner in combating cyber-related crimes on all levels, it would be natural to extend the cooperation to other regions or partners.

Cyber-exercises link international actors by using nodal governance to merge international security with the strategic and operational framework. These cyber-exercises are used to test organisations' ability to tackle a large-scale attack and resilience building. All of cyber-exercises are linked to cyber-strategies, as they set out the direction for cyber-operations (chapter 1). The European Networked Information Security Agency (ENISA) has launched international cooperation with the U.S. (EU-U.S. cooperation) to enhance the protection of CII against cyber-terrorism, i.e. the Cyber-Atlantic Exercise.[790] ENISA also launched a Cyber Europe 2014 exercise, where more than 200 organisations and 400 cyber-security professionals across Europe joined forces with twenty-nine EU and EFTA countries during the first phase of ENISA's bi-annual, large-scale cyber-security training. The members were called upon to resolve several scenarios that could influence the confidentiality, integrity or availability of sensitive information or critical infrastructures.[791] These exercises were considered a success, but it is impossible to get a clear overview of their effectiveness. The feedback is useful for detecting gaps in the existing legislative and technical framework.[792] However, this data is only communicated internally in the nodes, because detailed information regarding operations can endanger the whole security system. Therefore, the information remains confidential.

The EU is not alone to using these large-scale activities. NATO, held the largest exercise of its kind in 2013, with the aim of being able to prevent massively simultaneous attacks on the Member States and their allies. This organisation is state-centric in its foundation. However, the organisation reaches out to other actors and works in a nodal structure depending on the topic. To review, reinvent and progress their cyber-strategies, the alliance has included a number of technical experts, which proves

[789] EC (2011b) 'European principles and guidelines for Internet resilience and stability',10.
[790] ENISA (2011) 'Cyber Atlantic'.
[791] ENISA (2014a) 'Biggest EU cyber security exercise to date'.
[792]Sommestad and Hallberg (2012) 'Cyber security exercises and competitions as a platform for cyber security experiments',47.

that a form technification is integrated within the state-centric framework (sections 4.4, 4.5).[793] The aim of the exercise was to check NATO's and its partner's capability to technically and operationally respond to a large-scale cyber-attack, and review how efficiently participants coordinate their efforts.[794] The EU security actors could learn from NATO's operations, and vice versa. The lack of transparency and knowledge exchange on the strategic level is concerning, because progressing cyber-terrorism governance requires constant reviews of governance to capture the growing risks. Hopefully, feedback from these exercises is communicated back to the strategic level in order to improve the development of anticipatory governance forms and practices. Yet, nothing has been published, so I cannot include the effectiveness of cyber-governance and cooperation in the discussion.

6.5.2 The EU and Internal Cooperation

The EU cyber-security framework is attached to anticipatory governance, and this includes prevention, detection and response, as well as migration and recovery (section 3.7). Management requires a high level of coordination between the different nodes involved on a case-by-case basis, but also to other nodes that can learn from different experiences. Initiatives were launched towards CIIP in 2011. The new Directive proposal (2013) addresses insufficient level of harmonisation:[795]

> "[T]here is currently no effective mechanism at EU level for effective cooperation and collaboration and for trusted information sharing on NIS incidents and risks among the Member States. This may result in uncoordinated regulatory interventions, incoherent strategies and divergent standards, leading to insufficient protection against NIS across the EU".[796]

As highlighted in this 2013 document, the unbalanced regulatory level between the Member States can result in uncoordinated regulatory interventions, incoherent strategies and divergent standards, which can lead to insufficient protection against attacks.[797] I believe that there are tensions between how the different actors perceive the risks, in and from, cyber-space, which might create problems on the political/repose level (section 4.8.2). On one hand, there are problems related to state power, control and borders, which can be related to physical infrastructure and territorial sovereignty in relation to counter-terrorism.[798] On the other hand, in cyber-security tensions arise in

[793] Hansen and Nissenbaum (2009),1167. Garcia and Palhares (2014),277.
[794] RT(2013) 'NATO launches 'largest ever' cyber-security exercises'.
[795] EC (2013d),2.
[796] EC (2013d),3.
[797] EC (2013d),3.
[798] Dunn Cavelty (2013),117 - 118.

relation to networks, interconnectedness and the ability to self-govern in decentralised areas with many actors.[799] I argue that the development goes towards more cooperation across traditional boundaries and a wider participation of actors from both the public and the private sectors. This constitutes a significant break with the management of terrorism, which still upholds a very state-centric approach, which mirrors the original securitization approach. On reflection of this discussion, I believe that it is impossible to exclude the influence of the private actors in the development of cyber-security, because everybody is equally at risk. This creates tensions between the two different ways of seeing security, and the actors involved on the management level.

Appendix 7 outlines a broad range of EU security agencies working to enhance the resilience towards cyber-terrorism. Thus, I consider this a growing security area that will be systematised in the future. I would argue that is anticipatory governance is not only setting up obstacles to the cyber-risks, but also about increasing the development of resilience and preparedness and continuing to develop new response types. It is equally important to have responsive plans ready by imagining worst-case scenarios – or using hyper-securitization to capture the risks before they develop into threats (sections 3.7, 4.5.1).[800] The European Commission encourages Member States to develop national contingency plans and organise exercises simulating large-scale cyber-attacks, which can increase the security level, but also strengthen cooperation between national and international Computer Emergency Response Teams (CERT).[801] These are being created on EU, national and governmental levels to communicate information about risks and prevent cyber-attacks.[802] I uphold the argument that all these different actors and agencies increase the complexity of the cyber-security structure. Moreover, they fail to position the nodes in an organised way that can give a systematic overview of their functions, aims and interconnectivity. After a scrutiny of the documentary evidence, it is clear that information about the cooperative structures is missing, such as a comprehensive overview of participants, the foundation, and the aim and scope.

6.6 Cross-sectoral Cooperation

I have highlighted that in the nodal and anticipatory governance form, the interaction between sectors is likely to be formed by contractual cooperation rather than social

[799] Dunn Cavelty (2013),117-118.
[800] Hansen and Nissenbaum (2009).
[801] EC (2009c),2. EC/HREUFASP (2013),5.
[802] EC (2013c) ‘International digital agenda policy‘,6. EC/HREUFASP (2013),5.

obligations.[803] However, I find that the increasing use of PPPs goes beyond the traditional approach of market-based exchange of goods. Instead, it concerns voluntary participation towards a common goal (chapter 4).[804] PPPs are considered as a joint venture created to transfer knowledge and developing governance form regarding a particular security problem.[805] Cooperation of this kind is essential to increase resilience towards the risks imposed by hacktivists. The nodes are responsible to communicate information about their activities and achievements in order to reduce risks. In the past years, multifaceted attacks have been carried out by organisations, such as the Group Anonymous and LulzSec. These attacks have tweaked the interpretation of hacktivism and terrorism activities by being associated with highly mediated computer break-ins and the release of sensitive information as part of their global activities. Hacking groups, such as Group Anonymous and Lulzsec, are global organisations, but they are so loosely founded that the hacktivists do not necessary know each other (chapter 2 and 5).[806] It is important to create an extensive network on an ad hoc basis to manage this area.[807] It is not a matter of who is carrying out a speech act as Nissenbaum and Hansen claim.[808] Instead, it is important to establish the right combination of skills and knowledge, which can be communicated to the participants in the node - and pass on the information to relevant security actors, groups and individuals outside the node (chapter 5).

The governance structure is broadly founded to capture cyber-terrorism risks related to cyber-terrorism. This includes mobilising knowledge, capacity and resources of a variety of institutions, groupings and individuals. This has resulted in a cyber-governance structure that is much more complex than previously, because hybrid-constellations coexist with traditional forms of governance, and this creates a mixture of different types of governance and institutional arrangements (chapter 3). However, introducing PPPs in the context of cyber-terrorism is evident due to the security-level required and the complex technological risks. Both sectors bring invaluable knowledge of the cyber-security, but the private businesses add an important dimension to the cooperation due to their technology knowledge. The different nodes define and pursue their common interest in the cyber-security field, which has a long-term perspective

[803] Dunn Cavelty and Suter (2009) ‘Private-public partnerships are no silver-bullet’,2.
[804] Dunn Cavelty and Suter (2009),2.
[805] Linder (1999) ‘Coming to terms with the public-private partnership’,36.
[806] Dunn Cavelty (2013),113.
[807] Linder (1999),36.
[808] Hansen and Nissenbaum (2009). Garcia and Palhares (2014),276-277.

beyond administrating central plans or striving to meet alien objectives established outside the nodes.[809]

6.6.1 The EU's Public-Private Partnership

Combating cyber-terrorism requires a comprehensive strategy, and because of the nature of CI, CII and ICTs, the state-centric approach seems to be misplaced in a large number of hybrid security-constellations; mainly because PPPs are considered a relevant forum for progressing cyber-security through dialogue (section 5.6.3). The EU Commission has called for action to make Europe more prepared for, and resilient towards, cyber-disruptions and destruction. This form of public-private cooperation is characterised by various incitements for participating in the network and by the coexistence of trust and distrust originating in the tension between the different sectors (chapter 3).[810] I argue that the key area is, of course, to involve a group of actors with special knowledge that can establish a functional relationship in the nodes. However, I maintain that unlike Nissenbaum and Hansen's rethinking of securitization, this should not just combine state actors and some experts (section 4.5). Of course, these security actors are included in nodal governance, but they are just actors similar to others – and they do not hold a particular supreme position. Together the group of actors influence the security direction and pinpoint the actual needs of the public-private sectors, in order to close structural security gaps and to develop anticipatory governance. This can be done when different security actors combine their complementary strengths to increase their activities.[811]

The 2009 EU Communication on CIIP, for example, states that cross-sectoral cooperation is essential to address problems concerning CIIP. This document outlines the importance of establishing PPPs:[812]

> "To address this governance problem public-private partnerships (PPPs) have emerged at the national level as the reference model. However, despite the consensus that PPPs would also be desirable on a European level, European PPPs have not materialised so far. A Europe-wide multi-stakeholder governance framework, which may include an enhanced role of ENISA, could foster the involvement of the private sector in the definition of strategic public policy objectives as well as operational priorities and measures. This framework would bridge the gap between national policy-making and operational reality on the ground".[813]

[809] Loader and Walker (2007),133.
[810] Kock and Buser (2006),548.
[811] Schaeffer and Loveridge (2002),171.
[812] EC (2009b).
[813] EC (2009b),6.

Subsequently, the first formalised PPP in the European Framework followed the 2009 Communication, which brought the European Public-private Partnership for Resilience (EP3R) into the framework under the supervision of ENISA (2010).[814] Accordingly, the EU Communication (2011) increased the focus on PPPs and its role to progress resilience building of ICT infrastructures.[815]

> “The European Public-Private Partnership for Resilience (EP3R) was launched as a Europe-wide governance framework for the resilience of ICT infrastructures. It aims at fostering the cooperation between the public and the private sectors on strategic EU security and resilience policy issues […] EP3R will also serve as a platform for international outreach on public policy, economic and market matters relevant to security and resilience, in particular to strengthen the global risk management of ICT infrastructures”.[816]

The following EU Communication (2013) continued to develop a nodal and anticipatory governance framework by stressing the importance of a close relationship between public and private actors. Moreover, the communication explicitly emphasises several times that there is a shared responsibility to enhance the security of CI, CII and ICTs.[817] However, establishing an NIS private-public platform extends the framework beyond the mere management of the computer technologies related to CI and CII (chapters 2 and 5).[818]

6.6.2 Governance Structures

EP3R is divided into subunits characterised by working-groups that set out specific priorities. Before the establishment of EP3R, the lack of information exchange and expertise made prevention difficult because it was developed in closed structures without being communicated to a larger group of actors.[819] I believe the EU had sound intentions to improve the existing structure by establishing the PPPs - but in reality, this has been a very complicated process. The partnership acts as a supplement to the slow procedures in the established decision-making process. In this context, different governance forms and networks have obtained a significant position in introducing soft-approaches to the sectors (chapter 5). After analysing the data, I discovered that the reality does not live up to the intentions. I find it very disappointing that the slow process identified in chapter 5 continues because it creates weaknesses, not only in the legislative process, but also in alternative governance forms developed to close the legal

[814]ENISA (2014b) ‘European public private partnership for resilience (EP3R)’. EC (2009b)
[815] EC (2011a),5.
[816] EC (2011a),5.
[817] EC/HREUFASP (2013),5.
[818] EC (2013e).
[819] EC (2007b),7.

lacuna. By looking into EP3R, the progress of creating the partnership has been disturbingly slow, and this has results in the establishment of only two formalised PPPs within five years. It seems like the struggles with nodal governance is related not only to internal conflicts and tensions between the actors, but also the different systems, where the supranational bureaucratic systems needs to adjust to more flexible forms of cooperation.

The partnership also has other flaws. For example, the cooperation ought to go even further by involving different companies outside the scope of CII, which have extensive technical knowledge from developing preventive measures. This limitation is a mistake, because other actors can positively contribute to enhancing the knowledge of cyber-terrorism, technical innovations and management forms, which can be crucial to maximising security. Cyber-terrorism does not relate to one particular area, and there is not one particular method used to cause disruption or destruction. Net widening needs to be considered to give the partnership the breadth it requires. The scope of participation in the EP3R is too narrow to have significance, other than for the participating parties. This creates cognitive closed nodes where the security professionals are entwined in the cooperation without leaving space for new actors, which could bring new ideas for reinvention and rethinking of anticipatory procedures and governance practices (sections 3.3, 3.7, 4.8, 5.8). This creates a routinised application of security, which lacks the innovative dimension necessary to manage cyber-risks.[820]

The parties involved in EP3R are relevant national PPPs, appropriate public authorities, operators of communications networks, services and nodes, and relevant European (industry) associations.[821] I believe that the positive experience of Member States cooperating with the private sector and their roles and responsibilities have been transferred into this partnership. The consequences of the complex structure have forced the actors in EP3R to change the set-up by developing minor Task Forces. These Task Forces have been introduced to speed up the progress of developing the cooperation because the existing work groups were too slow.[822] Previously, it had taken too long to publish any visible outcome about these partnerships. The Task Force's reflect, analyse and draw conclusions on terminology definitions, trusted information sharing

[820] Bigo (2008),20.
[821] EC (2010h),9.
[822] EC (2007b),7.

mechanisms, mutual aid strategies, assess categorisation, incident management, tracking down botnets offenders, cyber-attack mitigation and response and a wide-scale and systematic malware disinfection.[823] By keeping the different groups small, the goal is to ensure a shorter time-scale in producing recommendations, greater flexibility in addressing current issues and prioritising the work, ensuring effective information sharing and better focus on their particular security issue.[824]

6.7 Accountability, Transparency and Openness in the Anticipatory Governance Framework

It is possible to bind this area to traditional counter-terrorism legislation, and therefore, there is a strong motivation for using securitization. However, this is concerning because it will circumvent the claim regarding more oversight, accountability and transparency in a negative way (sections 3.3.2, 4.8.3, 5.7). I argue that governmental accountability, transparency and openness are necessary tools for state representatives to inform society about their plans and actions. Of course, the actual behaviour and result of the activities can be subjected to public scrutiny, and sanctioned accordingly.[825] Accountability can only be upheld if the cyber-strategies and activities are at some point are made public, but only within the national state because there is no international oversight mechanism. I believe that the problem here is that large parts of counter-terrorism are securitized. Therefore, it is moved outside the normal democratic processes and covered by a high degree of secrecy (section 4.4). The Paris School is critical towards the dynamic between the security experts in transnational cooperation and their ability to develop exceptional measures as part of nodal governmentality. This internal development of self-governance is kept inside the nodes, which creates a field of (in)security due to the lack transparency and openness.[826] The lack of cyber-terrorism regulation means that the development of self-governance within the nodes is clearly open to an abuse of power, even if it is securitized or developed by security professionals within a closed nodal system. An example of this abuse of power can be seen in GCHQ's collection and exchange of meta-data, which has caused an international crisis in the confidence in security agencies. It is difficult to justify data collected from the German Chancellor's mobile phone and other EU representatives,

[823] EP3R (2013b) 'Work objectives',11. ENISA (2014b)'.
[824] EP3R (2013b),6.
[825]Eijkman (2012) 'Counter-terrorism, technology and transparency'. Ackerman (2005) 'Social accountability in the public sector'. Blind (2011) 'Accountability in public service delivery'.
[826] Bigo (2008),20.

when the justifications for data collection are meant to be security, terror, organised crime and economic well-being.[827]

6.7.1 Transparency and Openness and the Lack of Communication

The use of nodal governance side-steps the securitization process and seeks to create a different dynamic between the actors. This framework is thought to be flexible and heterogeneous in order to capture the different logic of experiences and practices deriving from the security actors. However, the Paris School has criticised this framework, perspective, claiming that this is precisely the problem with nodal governance where the actors do not convene to the same security understanding that generates internal struggles and differentiation.[828] The EU is trying to address these significant flaws in the structure. The Communication from 2009 reviewed the slow process of establishing the formalised PPPs.[829] Yet, I find it hugely worrying that a platform that was considered useful for improving governance, stalled because of too much bureaucracy, when that was exactly what it aimed to avoid. There are clear transparency problems concerning the procedures, the actors, aim and scope, and outcomes. It is noteworthy that the internal PPPs structure and communication are closed for public scrutiny and debate. I do understand that a certain level of secrecy is necessary to ensure security of the different areas. Yet, the closeness of the security nodes goes against EU legislation regarding the principle of openness and transparency and information to the citizens.[830] Articles 15 TFEU states that to promote good governance and ensure participation of civil society, the EU institutions, bodies, offices and agencies shall conduct their work as openly as possible.[831]

To succeed, it is important to create links to other security actors outside this environment, as it is equally important to direct communication by sharing findings with other nodes in order to develop a cycle of information sharing. It is to be hoped that the establishment of an NIS PPP addresses some of the issues that I have highlighted above. However, the NIS PPP is too broadly formulated to mandate cooperation specifically on CI, CII and ICTs. As a result, I think that it is difficult to predict how this will work out because nothing has been communicated regarding the

[827] MacAskill et al. (2013). Connolly (2013) ‘Angela Merkel: NSA snooping claims 'extremely serious'.

[828] Bigo (2008),12

[829] EC (2009b).

[830] Piris. Jean-Claude (2010),135,

[831] *Article 15 of the consolidated version of the Treaty on the functioning of the European Union.* Foster. Nigel (2010),24.

process.[832] Despite the novelty of this PPP, the experience with EP3R, has led one objective inbuilt in its foundation; the partnership needs to forward information by 2014.[833]

6.7.2 Attracting Private Actors to the EP3R

Following the discussion regarding the lack of transparency and openness, this PPP has other implications regarding participation and obtaining new knowledge from various sources. Attracting the correct security agents to EP3R is essential, and it is clearly a priority to attract high-level expertise from participants willing to allocate capabilities and resources.[834] It is not enough to create a technification, where security experts overtake the speech-act to persuade an audience to accept the securitization move.[835] The private sectors have extensive knowledge of CII and the use of technical measures to prevent cyber-terrorism, which are skills that the public sector lacks (chapter 5). For a long time, private companies have carried out threat assessments, established computer programmes and developed technical solutions to prevent cyber-attacks.[836] Their experience can be beneficial to other actors if shared. It is central to developing anticipatory governance and practices that the public sector receives information to formulate adequate and appropriate responses to the cyber- risks.[837] Moreover, I find it crucial that the governmental initiatives mirror the needs of the private sector in its decision-making process. Therefore, it is a win-win situation for all parties if the partnership progresses soundly. The challenge is to attract the right private actors to the cyber-security cooperation and to progress and share information rapidly beyond the nodes to enhance awareness about particular security concerns (chapters 3 and 5). Due to the limited number of publications regarding the PPP, it is not possible to say whether the EP3R has succeeded in attaching the relevant stakeholder. It seems more likely they have had a very turbulent time just establishing their aims and objectives, rather than worrying about who will be involved in the different nodes.

6.7.3 The Visibility and Outcome of the Cooperation

The aim of the PPP is to establish a European platform for cooperation, where the participants can develop good anticipatory governance and practices to prevent large-scale cyber-attacks. It is already established that this platform is faulty in many areas. It

[832] EC (2013e).
[833] EC (2013e).
[834] EC (2010h),10.
[835] Hansen and Nissenbaum (2009),1167. Garcia and Palhares (2014),277.
[836] EC (2007b),7.
[837] EC (2007b),7.

has been argued here that the overarching problems regarding accountability, transparency, and openness have stalled the development of the node, i.e. attracting security actors, communication beyond the node. The establishment of EP3R is progressing, and it has been doing so since 2009. It was recognised that in 2013, that it would be a key agency in the fight against cyber-attacks; yet, EP3R is far from reaching this objective.[838] In 2013, two reports were finally published, i.e. activities in 2012, and objectives for 2013.[839] The 2012 report outlines key findings and recommendations that establish the scope and the aims for the forthcoming work.[840] The first reports were released in 2013, the Activity Report 2012, and the Work Objectives 2013, which did not say much about the outcome and the cooperative partners.[841]

From the beginning, the nodal cooperation was tied up to thematic workshops on identified relevant topics and the establishment of working groups on the strategic level.[842] From 2011, it is possible to identify three working groups and their scope, but no data is available beyond this.[843] The aims and objectives of these working groups were described in very general terms, and there was surprisingly little information communicated to the public sphere. To address one of the problems, the Working Objectives 2013 set out an important goal, which could improve transparency and openness:

> "… [O]ne of the main objectives for EP3R is to regularly publish Position Papers on the ENISA Resilience Portal, once each Task Force has completed the various assignments. All position papers will be summarised in a yearly activity report".[844]

I find this claim about improving the publication rate rather interesting; ENISA's web portal reveals that three-positon papers were published on the 20th December 2013. However, this was the first publication, and nothing has been published since then.[845] This lack of communication is not surprising, but it is still very disappointing that an emerging security area, such as cyber-terrorism, is being neglected. Moreover, the

[838] EC (2010h),13.
[839] EP3R (2013a) 'Activity report 2012',5. EP3R (2013b),7.
[840] EP3R (2013a),14–20.
[841] EP3R (2013a), EP3R (2013b).
[842] EC (2010h),13.
[843] ENISA (2014b). EP3R (2011a) 'Working group 1'. EP3R (2011b) 'Working group 2'. EP3R (2011c) 'Working group 3'.
[844] EP3R (2013b),4.
[845] EP3R (2013) 'EP3R 2013', EP3R (2013c) 'Position paper of the EP3R Task Forces on incident management and mutual aid strategies' EP3R (2013e) 'Position paper of the EP3R Task Forces on trusted information sharing'.

reports lack visibility in the public sphere, and this complies with a significant part of the Paris School's critique.

Despite the best intentions in formalising the partnership, EP3R states in the Work Objectives report:

> "The proposed new structure of work takes advantage of the lessons learnt from the EP3R sessions held in 2010-2012, and addresses a number of shortcomings identified: unstable membership, long time-to-delivery, unclear priorities assigned to topics to address, insufficient buy-in from some members, etc.".[846]

These are serious flaws in the nodal structure, which harms the development of anticipatory governance and practices. Yet, I consider that the alternative is worse; a state-centric structure would be misplaced in order to manage this area. Nevertheless, I am inclined to state that a hierarchical structure might have been useful to establish the formal structure of the PPPs because the heterogeneous structure has proven to be inadequate to progress simple decision-making procedures. The partnership is a work-in-progress, but it is positive that they have finally recognised that they need a more flexible structure to deliver outcomes within a reasonable time. However, in the time that they have used to reach this conclusion, the virtual world has changed, and the problems of forming the PPPs have delayed the development of European anticipatory strategies – instead they have created a governance vacuum. The agency is organised without the proper oversight mechanism. It is formed under ENISA, so it is ENISA's responsibility to ensure that the work is progressing. However, from my analysis it looks like the agency has been left alone to establish its own foundation and no one is being held accountable for its lack of development. Issues regarding transparency and openness are a prevailing problem with ENISA. However, this should not be an area where there is any reason to keep information secret, because at this stage they have not even reached a point where they are discussing the development of governance forms.

6.8 Anticipatory Governance and the Development of Rules, Practices and Processes

When focusing on anticipatory governance to counter cyber-terrorism, it is necessary to direct the reader back to the previous chapter on cyber-security because the same reasoning applies to the development of anticipatory governance and regulatory practices under the European security framework. A mixture of rules, practices and processes are used as tools to maximise individuals and group's resilience to attacks. As

[846] EP3R (2013b),4.

I have illustrated in the ongoing security circle (figure 6), there are different anticipatory steps built into the risk-threat security circle. All of these different steps aim to capture the risks and later the threat, to prevent a catastrophic attack. However, different regulatory tools are being used to manage the risk of cyber-terrorism. Just as in the previous chapter, the development of anticipatory governance includes governmental rules, technical regulation, awareness-raising/education and self-defence/self-regulation. It is evident that the different governance forms are interrelated, and therefore, they are equally important in the management cycle.

6.8.1 State Regulation

The management of terrorism and cyber-terrorism requires differently regulatory initiatives in a mixture (section 5.8.1). The EU provides guidelines through programs, action plans and road maps for the Member States to implement in the domestic field. This gives the Member States a certain level of freedom and, at the same time, the guidelines provide for a harmonised security approach internally. However, in terms of protecting information systems, there is a lack of harmonisation between the Member States. To improve the legislative framework, the new 2013 Directive is adopted (section 5.5.2).[847] It is interesting that the Directive introduced specifically targeted legislation to prevent large-scale attacks against information systems – although it is not specified what kind of legislation it will cover. This aim of the Directive is ambiguous, in the sense that there are already severe problems with harmonising existing legislation. Moreover, the development of non-legislative measures has stalled in the PPPs, where they still struggle to develop a platform for communication.

This Directive covers purposes that are more important, such as strengthening critical information infrastructure protection and the removal of botnets (section 2.6).[848] It is highly relevant to include the different attack forms in the framework because they are an integral part of cyber-security. Especially as these botnets can pool enough servers together to enable attacks on essential CI, such as power plants, nuclear power stations, etc. (appendix 7):

> “This option provides for the introduction of specific targeted (i.e. limited) legislation to prevent large-scale attacks against information systems. Such strengthened legislation would be accompanied by non-legislative measures to strengthen operational cross-border cooperation against such attacks, which

[847] EC (2010a). EU (2013). EC (2014a) ‘Cybercrime’

[848] EC (2010a),3.

> would facilitate the implementation of the legislative measures. The aim of these measures would be to enhance the preparedness, security, and resilience of critical information infrastructure and exchange best practice”.[849]

Another important innovation is that the EU has finally recognised the need for developing supporting legislation to cover the lack of cyber-terrorism regulation and the legislative lacuna (section 5.4). The EU’s own bureaucratic procedures have confirmed its own inadequacy in providing an accurate level of protection, because the area is divided between counter-terrorism and cyber-crime legislation.

6.8.2 Technical Regulation

The implementation of technical regulation to avoid large-scale attacks is primarily based on governmental authority and responsibility. The private sector has a huge role in developing technical measures to secure computer networks and software, and to block cyber-terrorism (section 5.8.2). I maintain my previous claim, that through a wider cooperation between numerous stakeholders, it is possible to develop preventive technical security measures that strengthen the resilience towards cyber-terrorism attacks. Since the emergence of botnet, capacities to detect and monitor these nets have increased. I believe that the use of technical regulations requires close supervision, because a technical regulation constitutes a grey zone. This argument supports the concerns of the Paris School, who argue that security professionals can quickly fuel the insecurities of individuals through their routinised application of surveillance technologies, and through the use of technical equipment to filter and block Internet contents.[850]

Diverse measures can be used in the technical regulations, such as a form of self-regulation which requires authorisation to enter, monitor and record the utilisation of the system to detect activities, a periodic check of critical software, enforcing policies governing systems security and responding to attacks and unexpected events.[851] The measures are based on the technical capability to audit the system’s operation with the aim of detecting gaps in the computer-software, and discovering, preventing and investigating and incident afterwards. Nevertheless, more specific security procedures to prevent cyber-terrorism attacks are the responsibility of the individual computer

[849] EC (2010a),6.
[850] Bigo (2008),12.
[851] Lukasik et al. (2003) ‘Protecting critical infrastructure against cyber-attack’,18. Hawkins et al. (2000) ‘Awareness and challenges of Internet security’,132, 136.

users.[852] Technical measures used to prevent attacks improve the resilience by reducing the opportunities for hackers. This remains a balancing act, because it is easy to cross the boundaries between the public and private authority, and jurisdiction.

Continuously monitoring computer systems for signs of attacks and updating virus detection software regularly are just some of the means used.[853] Monitoring the Internet and assessing the security level is necessary in relation to cyber-terrorism, because DoS and DDoS are the preferred tools used to attack CI, CII and ICTs (appendix 5). Technical regulation does not only concern blocking, filtering and tracing Internet-traffic (section 5.8.2). Technical regulation is also concerned with the destruction of botnets, where technical security actors have an important role in dismantling botnets. For example, Internet service providers, Internet security companies, defence intelligence organisations, volunteer monitoring organisations and the academic community have all been instrumental in the dismantling of botnets (chapter 2).[854] It is, therefore, the area of anticipatory governance with the strongest links to the Copenhagen School's securitization, as this can easily be evoked in a limited space to prevent terrorism activities. Moreover, technical experts can have a convincing role in persuading an audience about the imminent urgency for action.[855] As mentioned before, the Turkey's Twitter case showed that there are problems of using securitization to manage the Internet, because the restrictions can easily be circumvented. Yet, I believe that the use of securitization is a part of a regulatory package included in the more comprehensive nodal governance approach, where the main focus is on anticipatory security forms and where securitization is evoked as a last resort.

6.8.3 Awareness-raising and Education

Awareness-raising and education are highly relevant to both the public and private sector (section 5.8.3). The recent focus on cyber-security by the mass media has profoundly helped to raise awareness of the risks of using cyber-space. It clearly draws attention to some massively overlooked areas in relation to cyber-terrorism, such as awareness-raising and education. Moreover, the attention of the mass media helps security actors to spread the preventive message of protection CII and ICTs, collectively

[852] Lukasik et al. (2003),18.
[853] Hawkins et al. (2000),131.
[854] Europol (2011c),8.
[855] Hansen and Nissenbaum (2009),1167. Garcia and Palhares (2014),277.

and individually.[856] However, ENISA did identify that a lack of awareness and education are two of the main problems, when they raised concerns about end-users' lack of knowledge regarding computer security. As a result, ENISA claims they could be more actively involved, and they state that the adoption of simple cyber-security measures by individuals would reduce the number of cyber incidents by 50% worldwide. However, this requires that the individuals are made aware of the risks and prevention forms.[857]

Awareness-raising, education, and training is areas where both the public and private sectors have essential roles to play in increasing the knowledge of cyber-risks. Individuals are the weakest link in the cyber-security. It is not enough to focus on the latest technology to protect against attacks. Individuals, employers and security actors can increase their risks by giving away information on social networks or by using their own, less secure, mobile devices.[858] Awareness-raising does not need to be created as a one-way communication. Keeping up a dialogue with the public is essential when understanding the development of cyber-terrorism. Communication forums can be formed as an exchange between security actors and individuals, where the individuals can pass on information about minor breakdowns, and suspicious information and behaviour online. In return, they can be informed about how to enhance their own security. I would argue that the Copenhagen Schools perspective on everyday practices is relevant to enhancing cyber-security. Computer users' experiences can be crucial for profiling and mapping cyber-terrorism, which decrease the uncertainty by identifying gaps and weaknesses in ICTs and the security framework.[859]

Primarily, governmental actors, institutional actors, professional security actors and the industry perform this in order to support a broad range of security initiatives. Training, for example, is highlighted in the joint EU Communication (2013):

> "Step up national efforts on NIS education and training, by introducing: training on NIS in schools by 2014; training on NIS and secure software development and personal data protection for computer science students; and NIS basic training for staff working in public administrations".[860]

[856] Caldwell (2013) 'Risky business'. Anderson (2013) 'How to safeguard your data in cyberspace'. Bradbury (2013) 'How to manage cyber-risks effectively'.
[857] ENISA (2013A) 'ENISA lists top cyber-threats in this year's threat landscape report'.
[858] Caldwell (2013).
[859] Hansen and Nissenbaum (2009),1165. Garcia and Palhares (2014),276.
[860] EC/HREUFASP (2013),8.

Security awareness includes the traditional forms of technical safeguards, such as firewalls, antivirus measures, user authentication, etc. Awareness-raising and education are also essential parts of the CERT Programme. The cyber risks are continually transforming, and the education and training material needs to be constantly reviewed in order to be up-to-date. This involves public and private participation in order to coordinate and design programmes directed towards current security risks, and to pinpoint the awareness and education necessary to mirror the needs of the different security actors.[861]

6.8.4 Self-defence and Self-regulation

The computer users are frontline security actors with the responsibility of securing their own computer systems (section 5.8.4). Rather than using the established counter-terrorism structure, discussions on self-defence and self-regulation are a significant step towards a more comprehensive cyber-security framework. This means that the Copenhagen School's perspective on securitization has no relevance in this area because they do not recognise the power of individuals to maximise security, except in the restricted role of passing on information.[862]

Self-governance is applicable to every computer user; including, governments, regional actors, the Internet provider, the software/hardware provider, user groups and individuals. As a result, it is necessary to widen the management-form and give the individual users a more prominent role in securing cyber-space, the Internet, search-engines, social media and chat forums. It can be argued that individuals are not direct targets of cyber-terrorism attacks, yet, they can have a role in attacks. The use of botnets, where large groups of users are involved, intentionally or unintentionally, in attacks, signifies the importance of involving this area in cyber-security.[863] Furthermore, it is important not to underestimate the role of cyber-space as a platform for propaganda and recruitment for a terrorist organisation. This is an integral part of the IS structure, where people react to the information flow from these web-pages. As long as the terrorists can see that this information has an influence on their cause, they will use the Internet as a platform for their global fight. Twitter and Google have tried to close down the online distribution of the beheading of hostages and other IS online propaganda. However, they have been caught up in their own bureaucracy and have been to slow to

[861] Hawkins et al. (2000),135.
[862] Hansen and Nissenbaum (2009),1165. Garcia and Palhares (2014),276.
[863] Europol (2011c),8

react. Google and Twitter’s problem is that their system is not developed to prevent the terrorist videos, hashtags and accounts getting online. Therefore, taking them offline has become a game of ‘whack-a-mole’, where as soon as they have removed the clip from one site, it will pop up on another site (section 2.6.3).[864]

Traditionally, there is a strict separation between private and public regulations. However, there is a movement towards a number of polycentric forms of governance, where the regulation is effected from a number of overlapping circles of power. This combines a horizontal concept of management by non-state security actors with the vertical multilevel governance, with interacting layers of public rules in international, regional, national and local levels.[865] The horizontal concept makes it difficult to exclude self-regulation and self-defence from the security framework. Europol’s Threat Assessment (2011) states that computer users and user groups are important actors.[866] The report states:

> “Users and user groups also have important roles to play in the prevention of Internet facilitated criminality, both at the individual and organisational level. Just as lack of public awareness and user neglect of security measures facilitate cybercrime, so too does an increased sense of online civic responsibility have the potential to reduce cybercriminal activity”.[867]

Although, there is a limited awareness of cyber-terrorism among individuals, this is an area which calls for more attention. The individual users can be active security actors within their limited space, even though they are not connected to security nodes or agencies. Through their online activates, individuals and groups can influence the actives and the behaviour in social media, the Internet, and cyber-space. Therefore, it is important to promote the development of ‘norms of behaviour’ in the virtual space, which stakeholders adhere to.[868]

6.9 Conclusion

Cyber-terrorism is a complex area to manage. Yet, it is progressing due to transnational and cross-sectoral cooperation, and the development of anticipatory governance forms. The Paris and the Copenhagen Schools’ security models have been useful for identifying security dimensions and strengthening the analysis. Although nodal

[864] Arthur (2014) ‘Taking down Isis material from Twitter or YouTube not as clear cut as it seems’. Gibbs (2014) ‘Islamic State moves to other social networks after Twitter clampdown’

[865] Koops (2008) ‘Criteria for normative technology’,161.

[866] Europol (2011c),9.

[867] Europol (2011c),9.

[868] EC/HREUFASP (2013),15.

governance is the preferred model for managing cyber-risks, it still causes problems in developing a comprehensive system based on anticipatory governance and practice introduced to increase resilience towards cyber-risks. I argue that this area is underdeveloped, and in the current form, it is caught between traditional counter-terrorism measures and cyber-crime governance forms. This creates an intellectual challenge for understanding the contradictory relationship between the two legislative frameworks. I also claim that the development of cyber-terrorism governance and practices is trapped between securitization and the use of nodal governance. It is clear that there is a problem regarding the lack of clearly formulated policies, and as a result, cyber-terrorism remains fragmented and differentiated. Moreover, on the surface, cyber-terrorism is in a limbo, where it is seen intrinsically as a state-centred concept.

The outcome of the documentary analysis is the confirmation that the governance of cyber-security is overwhelmingly based on a nodal structure, and this has a significant influence on how future cyber-risks are being addressed, including cyber-terrorism. Security actors overcome the gap in legislation and direct their focus on resilience building and protection of CI, CII and ICTs against cyber-attacks by developing anticipatory governance and practices. This is a positive development. However, it is not yet sufficient to create a coherent framework with effective safeguards and counter-measures because of limited data about the risks, constant technical innovations, a global playground, safe cyber-havens and the obstacles to counter-terrorism and cyber-crime measures (chapter 5). The documents I have analysed have highlighted that the regulatory governance forms discussed in the earlier chapters are included in European policy documents. Yet, because there is a significant lack of published impact assessments regarding anticipatory governance and practices in Europe, I can only conclude, that it could have been useful to include some evaluation of the effectiveness of these, and link it back to the theoretical work. However, as the information is missing, I am unable to assess whether the case studies, in practice, support the normative claim from the theoretical work on anticipatory governance.

There are still problems that need to be addressed. These relate to the slow process of developing and harmonising legislation to counter cyber-risks. The lack of communication between securities actors is critical and this cause accountability and transparency problems. These issues are a setback to the development of security measures and cooperation. In cross-sectoral cooperation, the idea of formalised PPPs is useful, and it creates an alternative structure to the state-centric cooperative form. Yet, I have identified serious transparency problems regarding the information flow. Moreover, accurate information is not available in the public sphere concerning future initiatives, objectives and topics, and the progress of the working groups already established. The issues mentioned above, makes it difficult to pin-point security measures directly towards vulnerable areas, and the lack of a comprehensive cyber-security framework is a significant obstacle to developing coherent anticipatory governance and practices.

7 The Understanding of Cyber-Security Governance and Practices in the European Region: The Concluding Chapter

7.1 The Research Objectives

This thesis has explored the dynamics and the complications of cyber-security strategies in European. It should be clear that cyber-security, cyber-crime, network security and defence strategies are some of the central governmental and security concerns of the 21st century. The revelations of former NSA contractor Edward Snowden underscore the importance security actors place in 'Mastering the Internet' in order to secure exclusivity of control over its infrastructure.[869] However, it is also clear that cyber risks are real, evolving, and potentially severe (section 1.1). These concerns create tension between ensuring the continued openness of the Internet and safeguarding it against dangers that may require re-assessment of societal expectations and practices.

As the technology evolves, as well as our expectations of what it can provide, there has been an asymmetrical evolution in the governance practices dedicated to cyber-security. Whereas security could once be discussed in specific terms, it has become more unclear because the capabilities of computing represent a paradigmatic shift in the potential scope and variety of vulnerabilities. These challenges pressures governments to close the growing gap between technological innovation and innovative nodal governance strategies for ensuring cyber-security. This chapter critically assesses European cyber-security governance strategies in order to increase the understanding of the area, and reflect on how can be improved. It will be a political and intellectual challenge to meet the future cyber-security concerns, decrease the complexity of nodal governance and accommodate the need for accountability, openness and transparency.

The overall research objective serves as the principal point for cyber-security. I have used them to utilise the understanding of anticipatory governance in European cyber-security strategies. I have addressed the research objective to enhance the understanding of a particular area, where I focused on anticipatory governance and practices to mandate cyber-risks. The chosen objective, which guided the reader through the different European cyber-security strategies and policies, enabled me to identify and understand the use of anticipatory governance in cyber-security, and the parameters included in the governance framework. Part one covered the theoretical foundation, which has been processed through a literature review, whereas the second part utilises

[869] MacAskill et al (2013b).

the theoretical basis for the substantial analysis. I believe that my examination of the concepts of cyber-security and cyber-terrorism have been useful in enhancing the understanding of nodal cooperation and its weaknesses (chapters 5 and 6).

In the first part of the thesis, I used the first sub-objective to evaluate the adequacy of the existing governance forms. These sub-objectives allowed me to create the necessary theoretical framework to further the discussion in part two. The analytical framework is progressed by a particular way of seeing the development of cooperation, as I have linked the different security paradigm to various international conflicts (sections 2.3, 2.4). It is clear that this creates a foundation for understanding, how and why cyber-security is managed in a particular way. This understanding has been significant in advancing the nodal and anticipatory discussion (sections 3.4, 3.7). Additionally, I have used the Copenhagen School and Paris School's theoretical perspectives to discuss and comment on the different parameters involved in cyber-governance (chapter 4). In the security and governance review, I have addressed the various aspects incorporated in cyber-security and the use of anticipatory governance. To progress this discussion, I have dedicated a part of chapter 4 to merging the theoretical knowledge of cyber-security with the substantive analysis in the second part.

In the second part of the thesis, I have employed the second sub-objective to investigate whether cyber-security strategies generate distinctive insights into growing cyber-challenges, i.e. cyber-security, and cyber-terrorism. I found that cyber-security covers a diverse and fragmented structure based on mixture of anticipatory governance and practices, and this constitutes a challenge for security actors. My analysis shows that there are serious gaps in the current governance structure, which are mostly linked to the complexity of the framework and the reluctance to collaborate worldwide. In this context, the research objective enabled me to investigate the substance of current security management, to highlight positive and negative elements in the structure, and to distinguish areas within the framework that need further attention.

7.2 The Contribution to Existing Knowledge

European cyber-governance and practices is an under-researched area, and the findings in this thesis give a meaningful understanding of anticipatory governance and practices developed to manage cyber-risks. I have identified four significant contributions on the existing knowledge regarding cyber-security. These four are linked to the European cyber-governance structure, where different issues have become visible during the analysis, and the originality derives from the governance gap in cyber-security literature (section 1.3). Firstly, I have linked the analysis to the concept of risk and anticipatory governance as the preferred security perspective in the 21st century. I am fully aware that there has been a lot written about risk in different sectors. However, the significance of this thesis is related to cyber-security and a specific way of thinking and responding to the growing online risks. These risks constitute political, institutional, strategic and intellectual challenges to understand the different parameters included in nodal and anticipatory governance. Secondly, I have primarily focused on the extensive European cyber-security framework introduced as a response to the growing cyber-space challenge. Thirdly, I have based the analysis on the increased use of multi-levelled cooperation, where the public-private dimension adds a different security dynamic to the framework. Fourthly, I have used Copenhagen School's reinvented securitization approach[870] and the Paris School's use of governmentality, to pinpoint weaknesses and critical security flaws in the anticipatory governance structure (chapters 5 and 6).[871]

7.3 The European Challenge of Cyber-security

The first contribution to the existing literature relates to Europe's cyber-security framework, and particularly, the EU's response to the cyber-security challenge (sections 1.2, 1.3, 4.7, 4.8, 6.9). I explored the contemporary European cyber-security challenges on the strategic level, because they are a precondition for developing and advancing the operational level. The insight into security strategies makes this area of research very interesting. Yet, it is an under-studied area globally, nationally and regionally. As a result, I would argue that the study is unique in its application of two distinct areas. Firstly, I have analysed the strategic level, which is an original contribution in itself. Secondly, I have directed my research at the European region, which is specifically overlooked in relation to cyber-security in academia. In Europe, a significant number of measures and governance forms have been developed and adopted, making Europe a suitable frame for this research. Nevertheless, the effort appears still fragmented and differentiated, and it has been impossible to get a proper overview of the initiatives launched because of the complicated nodal governance framework. It is, therefore, surprising that the European region has received such inadequate attention from within academia, who has instead chosen to focus on the U.S. response to cyber-risks,

[870] Hansen and Nissenbaum (2009),1163-1167. Garcia and Palhares (2014),276-277.
[871] C.A.S.E. Collective (2006),457. McDonald (2008b),570. Bigo (2008b),126.

computer law, national cyber-management or specific cyber-risks. More importantly, these areas are analysed on the operational level, e.g. preventive computer systems or technologies, data laws, particular cyber-risks or targets, surveillance and policing, filtering, blocking and censorship, or the right to privacy. Accordingly, in relation to the European framework, cyber-security research includes securitization, CI and CII, policing and surveillance. This thesis, however, offers a different perspective. I have chosen to investigate cyber-security strategies, and particular, European governance and practices, which opens up a new area of discussion. The following sections highlight the flaws in the governance structure, which were identified during the substantive analysis. These flaws are critically discussed in relation to the security perspectives of both the Copenhagen School and the Paris School.

7.3.1 Anticipatory Governance

The second research contribution to the existing literature derives from the predominant focus on risk-based security and anticipatory governance. By creating a risk-based framework based on anticipatory governance, I reject the use of threat-based theories and approaches, which has taken precedence in previous academic literature. There is a noteworthy gap in the literature concerning the differences between these two areas, and existing cyber-security research has failed to incorporate the use of European anticipatory governance into the security strategy discussion. Even though, risk and threat are part of the same logic, a certain level of uncertainty separates them, and existing security literature fails to make an explicit distinction between them. In cyber-security, risk is separated from the Copenhagen School's threat-based security perspective, whereas, the Paris School's management of unease is harder to define, because it can cover both a threat and risk (chapter 4).[872] Nevertheless, this thesis only includes anticipatory governance as the overarching concept, and by doing so, this study becomes distinctive compared to other cyber-security studies.

7.3.2 The Security Sectors

The third contribution to the existing literature positions public and private security actors equally within the security framework (chapters 2 to 6). The focus in existing research is mostly related to transnational cooperation, which thereby, overlooks a particular part of the security framework. In this context, cross-sectoral cooperation is equally important, and its combination with transnational cooperation creates a more

[872] Buzan et al (1998). C.A.S.E. Collective (2006),466.

comprehensive foundation for discussing and understanding cyber-security on the political and intellectual level. Research has only partially covered cross-sectoral cooperation, but this is primarily in relation to commercialised security and the use of private security contractors capitalising on cyber-security. In this thesis, I do not make any division between the different actors, because both public and private security actors face cyber-risks on an equal footing. Cyber-security constitutes a unique problem because of the way it continually develops due to the technological innovations, the skills of hackers, and its borderless space where ordinary rules and governance forms becomes inadequate. Moreover, every computer user is at risk of an attack and therefore, they have an obligation to prevent attacks by decrease vulnerabilities in their computer systems. Therefore, security collaboration broadens the framework to include multi-levelled security hybrids by combining state and non-state actors, but also by taking individual security actors seriously beyond everyday practices promoted by the Copenhagen School. I would argue that we only see the beginning of a more profound involvement of security actors outside state sectors. Actors, such as Microsoft, Apple, Google and Facebook, have increased their own involvement in cyber-security beyond the two sectors, and they will soon be the leading actors, which determine the security agenda.

7.3.3 The Security Approaches

The fourth contribution to the existing literature combines the reinvented securitization theory and governmentality in order to analyse cyber-security strategies. This is an unusual combination because Copenhagen School's securitization is primarily state-centric,[873] and Paris School's governmentality focuses primarily on the everyday management and security practices (sections 4.5, 4.6).[874] Despite the rethinking of securitization, it does not adequately encompass the way cyber-security is conducted despite the new addition of hyper-securitization, technification and every-day practices (section 4.5). The state-centric securitization process remains too restricted to embrace the complex and fragmented system embedded in cyber-security governance.[875] Yet, it is still possible to trace its former significance in transnational cooperation utilised by the state-centric security institutions, such as CoE and NATO. However, the EU is more inclined to breach the state-centric domination by involving numerous security actors in the framework. On the contrary, the Paris School perspective opens up to a more

[873] Buzan et al (1998),21. Sheehan (2005),53.
[874] Bigo (2008b),119, 127.
[875] Hansen and Nissenbaum (2009),1163-1167. Garcia and Palhares (2014),276-277.

inclusive security approach analysing internal power distribution between security actors.[876] Yet, the Paris School focuses too narrowly on the conduct of security professionals rather than particular understanding of how the different security dimensions are constructed and governed. The theoretical framework derives from the use of both approaches to give an empirical understanding, which has enabled me to critically assess European cyber-security policies, and review the application of those in the European region (chapters 5 and 6).

7.4 Conclusions and Normative Reflections

Anticipatory governance has an integral position in current security strategies (sections 3.7, 4.8, 5.8, 6.9). Despite the fact that this management form has been used widely, it needs to be more visible in policy-making by explicitly acknowledging the role of risk and pre-emptive activities that fall under the scope of anticipatory governance. The recognition of this management form is transferable to all parts of cyber-security on both the strategic and operational level. Accordingly, other security issues include anticipatory means on all levels, transnationally and cross-sectorally, such as drugs, trafficking, paedophilia, smuggling, money laundering, terrorism, cyber-crime and child abuse. Governance experience and exchange of knowledge from these traditional crime areas, as well as new emerging security problems, should be incorporated in the cyber-security structure. Security actors should also obtain governance-inspiration from related areas where artificial technologies are central, such as nano-technology, computing, artificial intelligence, biomedical, etc., because these share the same parameters and management concerns.

The development of governance forms and practices are based on the exchange of knowledge, and this should be promoted further to understand the way cyber-security is conducted, and whether the measures that have been introduced are useful. Without widespread communication, counter-measures will be inadequate to manage the evolving cyber-risks on a vertical and horizontal level because the different actors can learn from these consequences, irrelevant of whether they are related to successes or mistakes. Security actors' uncoordinated attempts will stand out as fragmented and incomprehensive and will fail to reach the predicted outcome. Therefore, the allocation of capabilities and resources should have a high priority on all security levels. This

[876] Bigo (2008b),119, 127.

requires that improvements be made to the security structure to facilitate a communication platform for distributing knowledge.

Creating a networked security framework is not without complications. A wide range of governmental and non-governmental actors needs to show a willingness to rethink existing security governance structures to improve the process and create synergy between the different initiatives. Despite tensions between the sectors, it will be beneficial for all parties, both at the managerial and operational level, to work towards defined goals. It is positive to see the EU advocating closer cooperation between public and private sectors through PPPs (sections 5.6. 6.6). Nevertheless, the clash between the supranational hierarchical system and flexible and cooperative nodal system slows down the development. This is a significant problem, which security actors need to address, and alternative governance forms needs to be in place to circumvent the traditional decision-making procedures. Moreover, the actors need to speed up their slow and bureaucratic processes. It is clear that this will require constant reviews and innovative thinking in developing alternative methods. The findings of this thesis have explicitly stated that cooperation is central. Exchange of knowledge on different levels should strengthen anticipatory governance processes and practices. Otherwise, the progress of cyber-security governance will stall due to regulatory failures, poor performances and communication deficits between the security agencies. The EU and CoE are important regional security actors that aim to secure, protect and stabilise the region. Nevertheless, they both need to improve external and internal cooperation where security actors seem to be reluctant to develop and harmonise legislation and governance through regional cooperation. Additionally, the public sector should be more open to collaborating with other sectors, organisations and individuals. Conversely, non-governmental security actors need to take more responsibility to address cyber-security challenges and participate in the cooperation.

Without doubt, the Paris and Copenhagen Security Schools have contributed to understanding the way cyber-security is drafted and the problem areas included in the framework. These two different approaches have made it possible to identify the weaknesses of a very complex nodal governance structure, and the influence it has on cyber-security. These problem areas identified in this analysis are related to the complexity of cooperation, the legislative lacuna, the lack of harmonisation, accountability and transparency, and the different governance forms included in anticipatory governance. These are areas, which need to be debated in order to create a comprehensive security framework. I argue that the cyber-security research contributes to the security agenda by identifying and recognising the current risk-security paradigm, and the parameters embedded in it. For example, I have examined how risk-management has moved beyond the securitization theory. Yet, there are parts of the new securitization interpretation, which are useful for the critical security analysis. Nonetheless, the thesis embeds cooperation and the development of anticipatory governance as the main topic, and this circumvents the explicit use of securitization. I will not reject the securitization approach, because it can be incorporated into the framework as part of an ongoing security management circle (figure 6). Due to the nature of cyber-security and the use of anticipatory governance, securitization cannot take precedence in the security framework, but it remains useful when other measures fail to capture the risks.

In the present security structure, security is not fixed to a particular referent object, but it is related to everything perceived as a risk, which depends on political, economic, and societal changes. I have shown that the risk-based security structure has more in common with the Paris School's focus on nodes, the interconnection between security professionals, and the development of self-governance forms (chapter 3 and 4).[877] Interaction and knowledge-exchange are placed centrally in cyber-security by involving multi-levelled security actors working in fragmented and diverse networks. This network structure is both an improvement and a problem for the region, because it rejects the pure state-centric understanding of security by creating a more comprehensive security framework by including external-internal actors and public-private sectors. However, nodal governance creates a very complicated and fragmented security structure, and it is difficult to fully to comprehend the numerous initiatives, regulations and networks developed (appendix 8).

I have used the two security schools as a foundation for investigating nodal governance based on anticipatory practices. As a result, I have divided the findings into four sub-areas, which covers the complexity of the structure, the legislative lacuna, accountability, and transparency, and anticipatory governance forms.

[877] Bigo (2008a),10.

7.4.1 The Complexity of Cyber-security

The findings of the research have shown that the cyber-security governance structures are very complex and fragmented. I find that it is nearly impossible to get a fully comprehensive overview regarding the actors, the purpose for cooperation and the organisation of the systems. Accordingly, the nodes are working in networked systems entwined in an extensive formation of a heterogeneous structure without one single primary node. This ensures the nodes have a high level of flexibility to enable them to restructure on a case-by-case basis. However, the nodal system is a problematic area for advancing cyber-security. Based on the findings, I am critical of the way security is conducted in nodes, the lack of openness and transparency, the unclear network structure and the failure to communicate knowledge to the public, such as naming participants, purpose, and the outcome of the cooperation (chapters 6 and 7). Moreover, this form of cyber-security governance is open to an abuse of power, because the strategies lack a clear overview of how to create and maintain oversight and accountability mechanisms within the structure. This is strongly interrelated to the lack of transparency and openness which is a direct result of the complexity.

This is a significant area, which is difficult to solve. On the one hand, security nodes must be created beyond traditional structures and alliances, and these nodes should be a function of a transnational and cross-sectoral level, involving stats, businesses, groups and individuals. I believe that it is necessary to enhance the existing framework to address the growing cyber-risks by requiring a platform for communicating knowledge, and sharing resources and capabilities, regardless of the actor's origins and belonging. On the other hand, these networked hybrids increase the complexity of the area, as there is little or no interaction between the nodes. I find it concerning that numerous nodes work in the same area without sharing vital information, and thereby, there is a risk that these actors overlook significant cyber-security problems due to the missing coordination between the security concerns. Moreover, there are only limited resources available to enhance the security framework, and these need to be distributed wisely between the actors. It is important to cast the net widely, but this will require that security actors are more open to sharing their knowledge and experience, which can improve the allocation of resources.

7.4.2 The Governance Lacuna

The adoption of cyber-security legislation follows lengthy procedures, and this creates an inadequate framework with a legislative gap. The legislation introduced is often faulty, outdated or incomprehensive, because the technology constantly develops. One example is the slow procedure of adopting the cyber-crime EU Directive (2013) (section 5.4), which still needs to be implemented by all the Member States.[878] Another example is the issue related to the CoE's Convention on Cyber-crime (2004), which is, to date, the only international cyber-crime agreement.[879] This treaty is already outdated, but it has never obtained an overwhelming international support, and therefore it appears unlikely that it will be updated. As a result, it remains insufficient for regulating the cyber-crime area. Additionally, attempts to create other international treaties have failed too (chapter 5). Finally, specific cyber-terrorism legislation has not been developed. Now, cyber-terrorism falls under two different sets of security regulations, i.e. counter-terrorism and cyber-crime, which complicates the development of comprehensive laws and governance forms for managing this particular area. Counter-terrorism and cyber-crime legislation and measures clash to some extent because counter-terrorism management is traditionally considered a state affair, and cyber-crime combines initiatives from both state and non-state actors. This would have been a larger problem in a pure state-centric application of security. However, in nodal governance, the state has a reduced role, by being a 'node among others'. As a result, non-legislative governance and practices overtake the area, and the power is distributed to a number of actors in the multi-levelled framework.

The slow legislative processes are a particular concern that needs to be addressed by security actors. I find this very worrying, and the division between the necessity of regulation, the lengthy process and the lack of a common stance seems unnecessary. Security actors from the different sectors should share the same motivation to create a functional framework, which is flexible enough to embed the changing cyber-risks. I am surprised that there are these significant harmonising and implementation problems regarding cyber-security initiatives, and this creates an unbalanced relationship between the different actors. Different countries within Europe have also shown an unwillingness to harmonise cyber-security governance and practices. As a result, the implementation progresses in a slow and inconsistent way, despite some improvements

[878] EC (2010a). EU (2013).
[879] CoE (2001).

being made within the EU (chapters 5 and 6). I claim that is a fundamental problem here. The European model is based on national states and the harmonisation of national legal regimes, etc. Harmonisation should be in the forefront of policy-makers' agenda, but the actors seem more concerned about internal disputes and power struggles, rather than to developing effective solutions. This is a real setback for developing a comprehensive cyber-security framework. Some states are pushing forward to improve the security level and introducing new governance forms, whereas others are less interested, and consider cyber-offences to be covered with ordinary legislation (chapters 4 to 6).

The same varying progress applies to the private sectors. Some actors might be involved because of a particular interest in improving cyber-security, while others see it as a way to capitalise on the security market, or influence decision-making (section 3.3, 4.8). It is problematic to obtaining knowledge about the private security actor's involvement in the security framework, unless these actors use it to brand themselves as necessary security actors, i.e. Microsoft, Apple and Google. It is also questionable how obliged the private security actors are to pass on their information and change their governance because of these cooperations. This challenges the intellectual and political understanding of how security is conducted in the 21st century. Finally, it is also difficult to get information about the information flow and the levels of communication which the private sector receives from other nodes to increase their security level.

7.4.3 Reliance on Different Governance Forms

There is a growing reliance on developing governance forms and rules, which outline good governance procedures to compensate for the lacking legislative framework. Moreover, new forms of cyber-related crimes are constantly emerging, which adds to the complexity of the management circle and significantly influences the predictability of future cyber-risks. This research has revealed that there are severe problems regarding harmonising and implementing the cyber-security initiatives developed in the region, and this creates an unbalanced relationship between the different states and actors. European countries have also shown an unwillingness to harmonise cyber-security and, as a result, the implementation progresses in a slow and inconsistent way, despite some improvements being made within the EU (sections 5.4, 6.5).

The findings in this thesis highlight the measured pace in which cooperation is developing. Accordantly, it looks like the security actors are scrambling around in the wilderness of different initiatives developed in a complex and fragmented framework. Transnational cooperation is the most developed area, because this has been a part of the security framework for decades (sections 2.3, 2.4). As a result, cooperative network areas are widely established compared with cross-sectoral cooperation. In this research, I have found that public-private cooperation is struggling to obtain a stronghold in the nodal governance structure (section 3.3). The introduction of formalised PPPs created the much-needed alternative to the lengthy legislative procedures and the state-centric security approach, which failed to include the non-state security dimensions in the framework (sections 5.6, 6.6). However, PPPs have proven equally averse to define and establish the cooperation - and to communicate with security actors. Surprisingly little information has been shared during the five years long process of establishing a formal PPPs in the EU. So far, the EP3R has failed, and it has exposed its own inadequacy in performing the simple task of setting up a forum for communication, and its failure to develop public-private processes, practices and guidelines to address the challenges of cyber-space.[880]

From an empirical perspective, it seems profoundly difficult to combine the bureaucratic and supernatural foundation of European institutions with the more flexible security partnerships. I find that there is an inadequate relationship between rationale for establishing PPPs and the practical development of the security dimension. If the broad security framework should succeed, the different actors need to accept that multilevel governance is the only alternative to the limited state-centric approach. Cyber-security should be positioned high on the agenda for all computer users, but there is a lack of awareness and knowledge regarding how to be involved in cyber-security and the possibilities to increase security on micro levels. It seems like many actors are interested in developing resilience and preparedness plans, but they struggle to coordinate the different initiatives.

7.4.4 Accountability and Transparency

The findings in this thesis have also exposed that there is a lack of communication and visibility in the public sphere. The way information is shared does not promote the necessary transparency and openness that could encourage groups and individuals to participate in a networked security structure. Moreover, the results of the

[880] ENISA (2014b). EC (2009b)

communication need to be shared with the public, in order to enlighten users about governance and practices, and ensure a certain level of security. By failing to provide a high standard of communication and publications, the security actors expose the efforts done to maximise security at different levels. Oversight and accountability systems are not explicitly mentioned in security strategies. This makes it difficult to hold anyone accountable for the failures in anticipatory governance policies, and it is only possible to use the democratic check and balance systems (sections 3.3.2, 4.8.3, 5.7, 6.7). This, of course, requires that the public be made aware of the governance forms, so that their legality can be questioned. If the public is unaware of the problems, or if it is impossible to reveal information due to the required level of secrecy, it becomes difficult to use the traditional democratic system. The findings in this thesis clearly outline that there are problems regarding the communication of anticipatory governance and practices. Additionally, cyber-space is global, and this limits the introduction of oversight and accountability mechanisms, unless they are explicitly outlined in the policy. Global and regional cooperation has proven to be a challenge, and the system is difficult to control. This makes it nearly impossible to keep security actors accountable for misconduct or illicit procedures, unless it is possible to challenge the actors' decisions in a particular jurisdiction. In the light of the Snowdon revelations in 2013, it should be in the interest of all security actors to improve accountability, openness and transparency. At the moment, there is a high level of scepticism linked to security actors. To overcome these problems, it is necessary to establish a fully functional governance framework, with a clear legislative base, a proper oversight mechanism and more transparency regarding the actors. As a result, they should communicate their aim and scope, the governance structure and the regulatory framework, and this would rebuild the trust in the security agencies. The long-term perspective is to include groups and individual in anticipatory governance and practices rather than being sceptical regarding the actors and their use of information.

7.4.5 Anticipatory Governance and Regulatory Practices

To improve anticipatory governance, I have identified four areas that are essential for developing a coherent cyber-security framework, i.e. state regulation, technical regulation, awareness-raising and education, and self-defence and self-regulation. As outlined above, the process of developing anticipatory governance is significantly problematic. Firstly, in terms of state-regulation, the effort is inconsistent and slow, and there are several legislative lacunas in the framework. Secondly, empirical observations of the development of technical regulation revealed the challenging relationship between the use of technological monitoring and the privacy of computer users. Due to the lack of communication between the security actors, internally and externally, it is hard to get an overview of the application of these measures to manage cyber-space. It is evidently used for surveillance and intelligence gathering, and the scale of date collection has created a debate about security actors' use of technical measures against citizens (as seen in the Snowden case). However, it is fascinating to observe the use of securitization, and the way security is framed to gain the legitimacy to use restrictive measures. For example, the securitization of Twitter in Turkey; this was done despite the lack of international consensus. Thirdly, the education of individuals and groups can be strengthened and integrated deeper into the security structure. Finally, self-defence and self-regulation are an overlooked part of the security framework, which, if activated and incorporated, can increase resilience. Previous cyber-security discussions have mistakenly left out this dimension, which has a significant influence on the governance of cyber-space (chapters 5 and 6). Regulatory practices developed by individual users are equally important to state and technical regulation, and it is a combination of all these regulation forms that creates a more comprehensive security dimension. The overarching challenge is to combine these regulatory governance forms and practices, which requires intellectual and political rethinking of security.

7.5 Future Research Areas

This concluding chapter does not mark the end of my research concerning the cyber-security governance and practices. Instead, this study has opened up further research areas which need to be explored. I have highlighted one important limitation to this thesis (section 1.4), which has to be addressed in future research. In future research, I will investigate the operational level to generate insight into cyber-security governance and its practicality. In addition, my research is focused on the security structures and strategies in the European region. However, I argue that the framework developed here could apply to international, national and local levels, because cyber-security governance and practices are entwined beyond the regional level. The reflections above reveal new avenues of research objectives which need to be drafted to cover a broad range of cyber-security problems. Future research could be extended to a specific cyber-security area, to analyse its particular governance forms. This area could be data protection, cyber-abuse and stalking, piracy, e-commerce, intellectual property, cyber-weapons, e-espionage, cyber-terrorism propaganda and recruitment, surveillance and control, blocking and filtering, organised crime, child abuse, social media and Internet communities, or economic crime and Internet transactions (chapter 6). Moreover, investigating accountability, transparency, and the role of security actors in cyber-security are prevalent and highly topical areas. Further research on the cyber-security paradigm could yield fruitful insights. For instance, the individual and private aspect of cyber-security could be further investigated. Thus, all of these research areas can create a foundation for more coherent risk-based cyber-security policies. To develop a research agenda, I have outlined seven recommendations that are useful to understand cyber-security beyond this thesis.

	Future research areas
Recommendation 1	**A key recommendation for future research would be empirical research on particular cyber-security problems, aimed at investigating security practices in action.**
Recommendation 2	**Progress the cyber-security framework further.** Further research is needed to create a sustainable framework for transnational and cross-sectored cyber-risks and the nature of cyber-space. More case studies in different cyber-security areas need to be analysed to create a coherent reflection of cyber-related security issues and governance.
Recommendation 3	**Develop an analytical framework for security governance in the 21st century**. Further research is needed which investigate the risk-security framework in other security areas. This research should encompass cooperation and the development of anticipatory governance. Future research should reflect on the way security strategies are formed and used in a nodal system beyond cyber-security.
Recommendation 4	**Examine specific nodal networks to enhance transnational and cross-sectored cooperation.** It is necessary to combine these two areas, i.e. transnational and cross-sectoral cooperation and examine the different forms of cooperation which have developed. The way transnational cyber-cooperation is developed is different from other security areas because management of cyber-space require a wide number of security actors. Moreover, the use of PPPs is an underdeveloped area that requires more attention.

Recommendation 5	**Examine accountability and transparency in security structures; eventually it will be possible to link this to more specific cyber-security areas.** Accountability and transparency structures are left out of current cyber-security strategies. Therefore, it is important to map oversight mechanisms and accountability in a hybrid-networked constellation with different security actors in transnational and cross-sectoral framework. It is important to look at the distribution of power internally in the nodes, the decision-making procedures and their external communication to the public.
Recommendation 6	**Further the investigation into exclusive anticipatory governance and practices imposed by cyber-security structures.** It is important to investigate the development of rules, practices and processes in other security areas. There is a need to look into governance processes and procedures to ensure further progress in risk-based security management. Particular research areas are state regulation, technical regulation, awareness raising and education, and self-defence/self-regulation.
Recommendation 7	**Examine the effectiveness of anticipatory governance and practices included in the European cyber-security framework.** This is a research area that is overlooked. In this thesis, I have investigated a range of practices/processes that are considered to be appropriate responses to threat/risk, in order to understand the security governance structure developed. However, due to the lack of data it was impossible to evaluate the success of these.

Table 3 future research areas

7.6 Final Remarks Regarding Future Research Areas

Some interesting research areas surfaced unexpectedly during my analyses which are not directly central to answering my research objective, but are essential for progressing the risk-based cyber-security framework in future research.

Firstly, the intellectual challenge of analysing security can be developed from this regional study. This thesis covers a limited part of cyber-security by focusing on the European region, with a conflicting state-centric and supranational system. The whole discussion regarding ‘security bureaucracy versus the heterogeneous structure’ forms an interesting constitutional problem.

Secondly, it could be interesting to replicate the analysis by using documents from other regions. A comparative study concerning Europe, North America, and Asia's cyber-security initiatives would be a remarkable option to progress the analysis from regional, political, social and/or constitutional perspectives.

Thirdly, a significant area emerged concerning the lack of separate cyber-terrorism regulations. This is particularly interesting because cyber-terrorism is considered a growing problem for both states and businesses, but it remains an overlooked legislative area. Cyber-warfare shares the same parameters as cyber-terrorism. Both are trapped between different regulatory frameworks, i.e. terrorism and cyber-crime legislation, warfare and cyber-crime legislation. Therefore, it could be interesting to extend the research to cyber-warfare.

Fourthly, the development of cyber-crime accelerates rapidly, and subsequently, the academic literature which focuses on this issue, quickly becomes outdated and irrelevant. As a result, I have included the use of mass media's coverage to get a substantive knowledge of cyber-attacks. Consequently, I would recommend investigating the influence of mass media in education and awareness-raising, and its significance in rethinking cyber-security.

Finally, the increasing inclusion of private actors, such as businesses and corporations, has revealed another research area. I want to investigate the motivation of individual actors to get involved in the security nodes. The private sector invests resources and knowledge, and this investment needs be beneficial to satisfy the market-oriented perspective. This fascinating element relates to the underpinning rationale for taking part in cross-sectoral cooperation, e.g. is this based on a genuine concern about cyber-security, to influence decision-making, brand themselves as security actors or is it a matter of promoting their business case? A combined qualitative and quantitative empirical study could be conducted in this area. These future research areas will be a guideline for developing a comprehensive understanding of cyber-security beyond this thesis.

8 Bibliography

Ackerman. J.M. (2005) 'Social Accountability in the Public Sector: A Conceptual Discussion', *Social Development Papers: Participation and Civic Engagement, 82 March, 2005.* >http://siteresources.worldbank.org/INTPCENG/214574-1116506074750/20542263/FINALAckerman.pdf<. [Accessed 21.07.2014].

Ackerman. Spencer (2014) 'Islamic State Militants Claim to have killed US journalist James Foley', *The Guardian. 20.08.2014. Webpage.* >http://www.theguardian.com/world/2014/aug/19/james-wright-foley-beheaded-isis-video<. [Accessed 04.09.2014].

Adams. John (1995) *Risk*. Routledge. Abingdon. United Kingdom.

Adey. Peter and Ben Anderson (2012) 'Anticipating Emergencies: Technologies of Preparedness and the Matter of Security' *Security Dialogue 2012 43:99.* >http://sdi.sagepub.com/content/43/2/99<. [Accessed 06.09.2013].

Agamben. Giorgio (2005) *State of Exception*. The University of Chicago Press. Chicago. United States.

Albert. Mathias and David Jacobson, Yosef Lapid (2001) *Identities, Borders, Orders. Rethinking International Relations Theory*, Minnesota University Press, Minnesota. United States.

Amoore. Louise and Marieke de Goede (2005) 'Governance, Risk and Dataveillance in the War on Terror' *Crime, Law & Social Change 2005 43, 149–173.* >http://link.springer.com/content/pdf/10.1007%2Fs10611-005-1717-8.pdf<. [Accessed 05.09.2013].

Amoore. Louise and Marieke de Goede (2008a) 'Introduction' (Ed.) Amoore. Louise and Marieke de Goede. *Risk and the War on Terror.* Routledge. Abingdon. United Kingdom**.**

Amoore. Louise and Marieke de Goede (2008b) *Risk and the War on Terror.* Routledge. Abingdon. United Kingdom.

Anderson. Ben (2007) 'Hope for nanotechnology: anticipatory knowledge and the governance of affect' *Area 2007 39:2, 156*-165. >http://onlinelibrary.wiley.com/doi/10.1111/j.1475-4762.2007.00743.x/pdf<. [Accessed 16.12.2014].

Anderson. Peter J. (1996) *The Global Politics of Power, Justice and Death, an Introduction to International Relations.* Routledge. Abingdon. United Kingdom.

Anderson. Tim (2013) 'How to safeguard Your Data in Cyberspace' *The Guardian. 11.02.2013. Webpage* >http://www.theguardian.com/media-network/media-network-blog/2013/feb/11/cyber-attack-data-mobile-security<. [Accessed 20.07.2014].

Ansell. Chris and Egbert Sondorp, Robert Hartley Stevens (2012) 'The Promise and Challenge of Global Network Governance: The Global Outbreak Alert and Response Network' *Global Governance 2012 18, 317-338, 317.* >http://heinonline.org/HOL/Page?handle=hein.journals/glogo18&div=30&g_sent=1&collection=journals#335<. [Accessed 20.07.2014].

Apps. Peter (2014) 'DDoS Cyber Attacks Get Bigger, Smarter, More Damaging' *Reuters. 05.03.2014. Webpage.* >http://www.reuters.com/article/2014/03/05/us-cyber-ddos-idUSBREA240XZ20140305<. [Accessed 25.08.2014].

Aradau. Claudia (2010) 'Security that Matters: Critical Infrastructure and Objects of Protection' *Security Dialogue* 2010 41:5, 491-514. >http://sdi.sagepub.com/content/41/5/491.short<. [Accessed 20.05.2015].

Aradau. Claudia (2014) 'The Promise of Security: Resilience, Surprise and Epistemic Politics' *Resilience* 2014 2:2,73-87. >http://www.tandfonline.com/doi/abs/10.1080/21693293.2014.914765<. [Accessed 20.05].

Aradau. Claudia and Rens Van Munster (2007) 'Governing through Risk: Taking Precautions, (Un)Knowing the Future' *European Journal of International Relations 2007 13:1, 89-115.* >http://ejt.sagepub.com/content/13/1/89.full.pdf+html<. [Accessed 20.08.2013].

Aradau. Claudia and Rens van Munster (2008) 'Taming the Future. The Dispositif of Risk in the War on Terror' (Ed.) Amoore. Louise and Marieke de Goede. *Risk and the War on Terror*. Routledge, Abingdon. United Kingdom.

Aradau. Claudia and Rens Van Munster (2009) 'Exceptionalism and the "War on Terror": Criminology meets International Relations' *British Journal of Criminology 2009 49, 686–701.* >http://bjc.oxfordjournals.org/content/49/5/686.full.pdf<. [Accessed 04.09.2013].

Aradau. Claudia and Rens van Munster (2011) *Politics of Catastrophe: Genealogies of the Unknown*. Routledge, Abingdon. United Kingdom.

Aradau, Claudia and Luis Lobo-Guerrero, Rens Van Munster (2008) 'Security, Technologies of Risk, and the Political: Guest Editors' Introduction' *Security Dialogue* 2008 39:2/3, 147. >http://bigo.zgeist.org/students/readings/IPS2011/12/aradau%20van%20munster%202008%20Sec%20dial ogue.full.pdf<. [Accessed 22.05.2015].

Arribas-Allyon. Michael and Valerie Walkerdine (2008) 'Foucauldian Discourse Analysis' (Ed.) Willig. Carla and Wendy Stainton-Rogers (2008) *The SAGE Handbook of Qualitative Research in Psychology*. Sage Publication. London. United Kingdom.

Arthur. Charles (2013) 'Internet Slows Down after DNS Attack on Spamhaus' *The Guradian. 28.03.2013. Webpage.* >http://www.theguardian.com/technology/2013/mar/27/cyber-attack-spamhaus-slows-down-internet<. [Accessed 27.07.2014].

Arthur. Charles (2014) 'Taking down Isis material from Twitter or YouTube not as clear cut as it seems' *The Guardian, 23.06.2014. Webpage.* >http://www.theguardian.com/world/2014/jun/23/taking-down-isis-youtube-twitter-google-video<. [Accessed 04.09.2014].

Aquilina. Kevin (2010) 'Public Security versus Privacy in Technology Law: A Balancing Act?' *Computer Law and Security Review 2010 26, 130-143.* >http://www.sciencedirect.com/science/article/pii/S0267364910000166<.[Accessed 12.12.2014].

Arquilla. John and David Ronfeldt (1993) 'Cyberwar is Coming' *Comparative Strategy 1993 12:2, 141–165.* >http://www.tandfonline.com/doi/pdf/10.1080/01495939308402915<. [Accessed 21.04.2013].

Arquilla. John and David Ronfelt. (1999) The Emergence of Noopolitik: Toward an American Information Strategy. *Rand Corporation. Washington DC. United States*. >http://www.rand.org/pubs/monograph_reports/MR1033.html<. [Accessed 16.12.2014].

Arquilla. John and David Ronfeldt (2001) *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Rand Corporation. Sana Monica, Arlington. Pittsburg. United States.

Avant. Deborah D. (2005) *The Market for Force: The Consequences of Privatizing Security*. Cambridge University press. Cambridge. United Kingdom.

Avina. Jeffery (2011) 'Public-private Partnerships in the Fight against Crime. An Emerging Frontier in Corporate Social Responsibility' *Journal of Financial Crime* 2011 18:3, 282-291. >http://search.proquest.com/docview/877023580/fulltextPDF?accountid=12253<. [Accessed 08.09.2013].

Ayers. Ian and John Braithwaite (1992) *Responsive Regulation**:** Transcending the Deregulation Debate.* Oxford University Press. Oxford. United Kingdom.

Ayoob. Mohammad (1995) *The Third World Security Predicament: State Making, Regional Conflict and the International System*. Lynne Rienner. Boulder. United Kingdom.

Ball. James and Julian Borger, Glenn Greenwald (2013) 'Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security' The Guardian. *The NSA Files. Webpage.* >http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security<. [Accessed 10.12.2014].

Barben. Daniel, and Erik Fisher, Cynthia Selin, David H Guston. (2008) 'Anticipatory Governance of Nanotechnology : Foresight, Engagement, and Integration' (Ed.) Hackett. Edward. J. and Olga Amsterdamska, Michael Lynch, Judy Wajcman (2008) *The Handbook of Science and Technology Studies*. MIT Press. Cambridge, United Kingdom. >http://www.hks.harvard.edu/sdn/articles/files/Barben-STS_Handbook-Anticipatory_Governance_Nanotechnology-08.pdf< . [Accessed 21.12.2014].

Barber. Richard (2001) 'Hacker' Profiled – Who Are They and What Are Their Motivations?' *Computer Fraud & Security 2001 2, 14–17.* >http://www.sciencedirect.com/science/article/pii/S1361372301020176<. [Accessed 20.12.2014].

Barlow. John Perry (1996) 'A Declaration of the Independence of Cyberspace' *Webpage.* >http://wac.colostate.edu/rhetnet/barlow/barlow_declaration.html<. [Accessed 20.08.2014].

Barnard-Wills. David and Debi Ashenden (2012) 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk' *Space and Culture 2012 15:2, 110-123.* > http://sac.sagepub.com/content/15/2/110.full.pdf+html<. [Accessed 23.01.2015].

Barry. Andrew and Thomas Osborne, Nicolas Rose (1993) *Economy and Society Special Issue on Liberalism and Governmentality.* Routledge. London. United Kingdom.

Bartle. Ian and Peter Vass (2007) **'**Self-regulation within the Regulatory State: Towards a New Regulatory Paradigm?' *Public Administration 2007 85: 4, 885-905.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1467-9299.2007.00684.x/pdf<. [Accessed 08.09.2013].

Batty. David (2012) 'Vatican Becomes Latest Anonymous Hacking Victim' *The Guardian. 07.03.2012. Webpage.* >http://www.theguardian.com/technology/2012/mar/07/vatican-anonymous-hacking-victim<. [Accessed 27.07.2014].

Brassett. James, and Nick Vaughan-Williams (2015) 'Security and the Performative Politics of Resilience: Critical Infrastructure Protection and Humanitarian Emergency Preparedness'. *Security Dialogue* 2015 46:1, 32-50. >http://sdi.sagepub.com/content/46/1/32.short<. [Accessed 25.05.2015].

Bauman. Zygmunt and Bigo, Didier, Paolo Esteves, Elsbeth Guild, Vivienne Jabri, David Lyon, R.B.J. Walker, (2014) 'After Snowden: Rethinking the Impact of Surveillance' *International Political Sociology, 2014 8:2, 121-144.* >http://onlinelibrary.wiley.com/doi/10.1111/ips.12048/full<. [Accessed 10.11.2014].

Bayley. David and Clifford Shearing (2001) The New Structure of Policing: Description, Conceptualization, and Research Agenda. *National Institute of Justice. Washington DC. United States*.

BBC News (2007) 'Estonia Hit by 'Moscow Cyber War' *World. 17.05.2007. Webpage*. >http://news.bbc.co.uk/1/hi/world/europe/6665145.stm<. [Accessed 12.09.2013].

BBC News (2009) 'Governments Hit by Cyber Attack' *Technology. 08.07.2009. Webpage*. >http://news.bbc.co.uk/1/hi/technology/8139821.stm<. [Accessed 21.04.2013].

BBC News (2010a) 'Anonymous Hacktivists say WikiLeak War to Continue *News. 09.12.2010. Webpage*. >http://www.bbc.co.uk/news/technology-11935539<. [Accessed 12.09.2013].

BBC News (2010b) 'Burma Hit by Massive Attack ahead of Election' *Technology. 04.11.2010. Webpage*. >http://www.bbc.co.uk/news/technology-11693214<. [Accessed 09.09.2013].

BBC News (2010c) 'Google in 'New Approach' in China' *Business. 30.06.2010. Webpage.* >http://www.bbc.co.uk/news/10443648<. [Accessed 12.09.2013].

BBC News (2010d) 'Pro-Wikileaks Activists Abandon Amazon Cyber Attack' *Technology. 09.12.2010. Webpage.* >http://www.bbc.co.uk/news/technology-11957367<. [Accessed 12.09.2013].

BBC News (2011a) 'Japan Defence Firm Mitsubishi Heavy in Cyber Attacks' *Asia-Pacific. 20.09.2011. Webpage.* >http://www.bbc.co.uk/news/world-asia-pacific-14986694<. [Accessed 21.04.2013].

BBC News (2011b) 'South Korea Hit by Cyber Attacks' *Technology. 04.04.2011. Webpage.* >http://www.bbc.co.uk/news/technology-12646052<. [Accessed 09.09.2013].

BBC News (2012a) 'Anonymous Hacker Group Attacks Israeli Websites' *Technology. 16.11.2012. Webpage.* >http://www.bbc.co.uk/news/technology-20356757<. [Accessed 12.09.2013].

BBC News (2012b) 'Chinese websites 'defaced in Anonymous attack' *News. 05.04.2012. Webpage.* >http://www.bbc.co.uk/news/technology-17623939<. [Accessed 26.07.2014].

BBC News (2012c) 'Hackers had 'Full Functional Control' of Nasa Computers' *Technology. 02.03.2012. Webpage.* >http://www.bbc.co.uk/news/technology-17231695<. [Accessed 09.09.2013].

BBC News (2012d) 'Syria Conflict: West 'Appalled' by Russia China UN Veto' *News. 19.07.2012. Webpage.* >http://www.bbc.co.uk/news/world-middle-east-18914578<. [Accessed 09.09.2013].

BBC News (2012e) 'The Hacking Group Anonymous Says it will Launch Online Attacks Every Weekend, Following Claims it Disrupted Access to the Home Office Website' *News. 08.04.2012. Webpage.* >http://www.bbc.co.uk/news/uk-17648852<. [Accessed 20.07.2014].

BBC New (2012f) 'Wikileaks Websites Back Online after DDoS Cyber Attacks' *Technology. 12.08.2012. Webpage*. >http://www.bbc.co.uk/news/technology-19255026<. [Accessed 09.09.2013].

BBC News (2013a) 'Adobe in Source Code and Customer Data Security Breach' *Technology, 18.10.2013, Webpage.* >http://www.bbc.co.uk/news/business-24392819<. [Accessed 11.08.2014].

BBC News (2013b) ‘Apple Moves to Close Java Hack Flaw after Intrusion’ *Technology. 20.02.2013. Webpage.* >http://www.bbc.co.uk/news/technology-21519856<. [Accessed 11.08.2014].

BBC News (2013c) ‘Australia's Central Bank Targeted by Hackers’ *Businesses*. *11.03.2013. Webpage.* >http://www.bbc.co.uk/news/business-21738540<. [Accessed 11.07.2013].

BBC News (2013d) ‘Australia Sites Hacked amid Spying Row with Indonesia’ *News. 21.11.2013. Webpage.* >http://www.bbc.co.uk/news/world-asia-25029261<. [Accessed 26.07.2014].

BBC News (2013e) ‘Cyber Attack Hits South Korea Websites’ *Asia. 20.06.2013. Webpage*. >http://www.bbc.co.uk/news/world-asia-23042334<. [Accessed 11.07.2013].

BBC News (2013g) ‘NatWest Online Services hit by Cyber Attack’ *News. 06.12.2013. Webpage.* >http://www.bbc.co.uk/news/business-25262790<. [Accessed 26.07.2014].

BBC News (2013h) ‘NatWest Cyber Attack Disrupted Ulster Bank Website’ *News. 06.12.2013. Webpage.* >http://www.bbc.co.uk/news/uk-northern-ireland-25269930<. [Accessed 26.07.2014].

BBC News (2013i) ‘Kent Man Admits Oxbridge and Police Force Cyber Attacks’ *News. 15.04.2013. Webpage*. >http://www.bbc.co.uk/news/uk-england-22149435<. [Accessed 11.07.2013].

BBC News (2013j) ‘South Korea Network Attack ‘a Computer Virus’’ *Asia*. *20.03.2013. Webpage.* >http://www.bbc.co.uk/news/world-asia-21855051<. [Accessed 10.09.2013].

BBC News (2013k) ‘Wall Street Journal ‘also Victim of China Hacking Attack’ *China. 31.01.2013. Webpage.* >http://www.bbc.co.uk/news/world-asia-china-21287757<. [Accessed 21.04.2013].

BBC News (2014a) ‘North Korea Refuses to Deny Sony Pictures Cyber-attack’. *Asia. 02.12.2014. Webpage.* >http://www.bbc.co.uk/news/world-asia-30283573<.

BBC News (2014b) ‘Russia Gang Hacks 1.2 Billion Usernames and Passwords’ *Technology*. *06.08.2014. Webpage.* >http://www.bbc.co.uk/news/technology-28654613<. [Accessed 11.08.2014].

BBC News (2014c) ‘Sony Hack: White House views Attack as Security Issue’ *US and Canada. 19.12.2014. Webpage.* >http://www.bbc.com/news/world-us-canada-30538154<.

BBC News (2014d) ‘Sony Pictures Computer System Hacked in Online Attack’ *Technology*. *25.11.2014. Webpage*. >http://www.bbc.co.uk/news/technology-30189029<.

BBC News (2014e) ‘South Korea to Develop Stuxnet-like Cyberweapons’ *News. 21.02.2014. Webpage.* >http://www.bbc.co.uk/news/technology-26287527<. [Accessed 17.07.2014].

Beck. Ulrich (1992) *Risk Society. Towards a New Modernity*. Sage Publications. London. United Kingdom**.**

Beck. Ulrich (1994) ’The Reinvention of Politics: Towards a Theory of Reflexive Modernization’ (Ed.) Beck. Ulrich and Anthony Giddens, Scott Lash. *Reflexive Modernization. Politics, Tradition and Aesthetic in the Modern Social Order.* Polity Press. Cambridge. United Kingdom.

Beck. Ulrich (1995) *Ecological Politics in an Age of Risk*. Polity Press. Cambridge. United Kingdom.

Beck. Ulrich (1999) *World Risk Society*. Polity Press. Cambridge. United Kingdom.

Beck. Ulrich (2002) ’The Terrorist Threat. World Risk Society Revisited’ *Theory Culture Society 2002 19:4, 39-55.* >http://tcs.sagepub.com/content/19/4/39.full.pdf<. [Accessed 06.09.2013].

Beck. Ulrich (2006) ‘Living in the World Risk Society’ *Economy and Society 2006 35: 3, 329-345.* >http://www.tandfonline.com/doi/pdf/10.1080/03085140600844902<. [Accessed 06.09.2013].

Beck. Ulrich (2009) *World at Risk*. Polity Press. Cambridge. United Kingdom.

Beken. Tom Vander and Kristof Verfaille (2010) ’Assessing European Futures in an Age of Reflexive Security’ *Policing and Society: An International Journal of Research and Policy 2010 20:2, 187-203.* >http://www.tandfonline.com/doi/pdf/10.1080/10439461003721242<. [Accessed 09.09.2013].

Bellamy. Alex J. (2004) International Society and its Critics. Oxford University Press. Oxford. United Kingdom.

Bellamy. Alex J. and Matt McDonald (2002) ‘The Utility of Human Security': Which Humans? What Security? A Reply to Thomas & Tow’ *Security Dialogue 2002 3:3, 373-377.* >http://sdi.sagepub.com/content/33/3/373.full.pdf+html<. [Accessed 13.12.2014].

Bendrath. Ralf and Johan Eriksson, Giampiero Giacomello (2007) ‘From’Cyberterrorism’to’Cyberwar’ Back and Forth’ (Ed.) Eriksson. Johan und Giampiero Giacomello (2007) *International Relations and Security in the Digital Age.* Routledge. Abingdon. United Kingdom.

Bendrath. Ralf (2001) ‘The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection’ *Information & security 2001 7, 80-103.* >http://directory.cip.management.dal.ca/publications/Cyberwar%20debate%20-%20perceptions%20and%20politics.pdf<. [Accessed 01.02.2015].

Betts. Richard K. (1997) ‘Should Strategic Studies Survive?’ *World Politics, 1997 50:01, 7-33.* >http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=7659732&fileId=S0043887100014702<. [Accessed 20.12.2014].

Bevir. Mark and Roderick Arthur William Rhodes (2003) *Interpreting British Governance*. Routledge. London. United Kingdom.

Bigo. Didier (2001) ‘The Möbius Ribbon of Internal and External Security(ies)’ (Ed.) Albert. Mathias and Yosef Lapid, David Jacobson (2001) *Identities, Borders, Orders*. University of Minnesota Press, Minnesota. United States. >http://www.academia.edu/3102803/The_M%C3%B6bius_ribbon_of_internal_and_external_security_ies_<. [Accessed 20.12.2014].

Bigo. Didier (2000) Liaison Officers in Europe: New Officers in the European Security Field (Ed.) Sheptycki. James (2000) *Issues in Transnational Policing.* Routledge. Abingdon. United Kingdom.

Bigo. Didier (2002) ‘Security and Immigration: Toward a Critique of the Governmentality of Unease’ *Alternatives: Global, Local, Political 2002 27:1, 63-92.* >http://alt.sagepub.com/content/27/1_suppl/63.citation<. [Accessed 02.06.2014].

Bigo. Didier (2006a) ’Internal and External Aspects of Security’ *European Security 2006 15:4, 385-404.* >http://www.tandfonline.com/doi/pdf/10.1080/09662830701305831<. [Accessed 03.09.2013].

Bigo. Didier (2006b) ‘Protection: Security, Territory and population’ (Ed.) Huysmans. Jef and Andrew Dobson, Raia Prokhovnik (2006) *The Politics of Protection, Sites of Insecurity and Political Agency*. Routledge. London. United Kingdom.

Bigo. Didier (2008a) ‘Globalized (In)Security. The Field and the Ban-opticon’ (Ed.) Bigo, Didier and Anastassia Tsoukala. *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes after 9/11.* Routledge. Abingdon. United Kingdom.

Bigo. Didier (2008b) ‘International Political Sociology’ (Ed.) Williams. Paul. D. *Security Studies: An Introduction.* Routledge. Abingdon. United Kingdom.

Bigo. Didier (2008c) ‘Security. A Field Left Fallow’ **(**Ed.) Dillon. Michael and Andrew W. Neal. *Foucault on Politics, Security and War.* Palgrave MacMillan. Basingstoke. United Kingdom.

Bigo. Didier and Anastassia Tsoukala (2008) ‘Understanding (In)Security’ (Ed.) Bigo, Didier and Anastassia Tsoukala. *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes after 9/11.* Routledge. Abingdon. United Kingdom.

Bigo. Didier and Sergio Carrera, Elspeth Guild, R.B.J. Walker (2009) ‘The Challenging Landscape of European Liberty and Security: The Mid-term Report of the CHALLENGE Project’ *UNESCO 2009*. Blackwell Publishing. Oxford. United Kingdom.

Bigo. Didier and Emmanuel-Pierre Guittet (2011) ‘Northern Ireland as Metaphor: Exception, Suspicion and Radicalization in the ‘War on Terror’’ *Security* Dialogue 2011 42:6, 483-498. >http://sdi.sagepub.com/content/42/6/483.full.pdf+html<. [Accessed 04.09.2013].

Bigo. Didier and Gertjan Boulet, Caspar Bowden, Sergio Carrera, Elspeth Guild. Nicholas Hernanz, Paul de Hert, Julien Jeansesboz, Amandine Scherrer (2013) ‘Open Season or Data Fishing on the Web. The Challenges for the US prism Programme for the EU’ *CEPS POLICY BRIEF No. 293, 18 June 2013.* >http://www.ceps.eu/book/open-season-data-fishing-web-challenges-us-prism-programme-eu<. [Accessed 10.12.2014].

Black. Julia (2002) ‘Critical Reflections on Regulation’ *Australian Journal of Legal Philosophy 2002 27:1, 1-36.* >http://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/ajlph27&div=4&id=&page=<. [Accessed 08.09.2013].

Blind. Pagek (2011) ‘Accountability in Public Service Delivery: A Multidisciplinary Review of the Concept’, *Expert Group Meeting Engaging Citizens to Enhance Public Sector Accountability and Prevent Corruption in the Delivery of Public Services, Vienna, Austria 1-8 & 11-13 July 2011.* >http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan046363.pdf<. [Accessed 21.07.2014].

Blum. Andrew (2012) ‘Tubes, A Journey to the Centre of the Internet’ *Fresh Air. Webpage.* >http://www.npr.org/2012/05/31/153701673/the-internet-a-series-of-tubes-and-then-some<. [Accessed 15.12.2014].

Bonditti, Philippe (2004) ‘From Territorial Space to Networks: A Foucauldian Approach to the Implementation of Biometry’ *Alternatives: Global, Local,* Political 29 (4): 465–482. >https://www.questia.com/library/journal/1G1-126318199/from-territorial-space-to-networks-a-foucaldian-approach<. [Accessed 08.01.2015].

Booth. Ken (1997) ‘Security and Self: Reflections of a Fallen Realist’ (Ed.) Krause. Keith and Michael Williams. *Critical Security Studies*. University of Minnesota Press. Minnesota. United States.

Booth. Ken (2004) ‘Critical Security Studies and World Politics’ (ed.) Lynne Rienner Publishers Inc. London. United Kingdom

Booth. Ken (2007) *Theory of World Security*. Cambridge University Press. Cambridge. United Kingdom.

Borodzicz. Edward P. (2005) *Risk, Crisis & Security Management*. Wiley. Southern Gate. United Kingdom.

Bos. Wilfried. and Christian Tarnai (1999) ‘Content Analysis in Empirical Social Research’ *International Journal of Educational Research 1999 31:8, 659–671.* >http://www.sciencedirect.com/science/article/pii/S0883035599000324#<. [Accessed 25.08.2013].

Bovens. Mark (1998) *The Quest for Responsibility: Accountability and Citizenship in Complex Organisations* Cambridge University Press. Cambridge. United Kingdom.

Bovens. Mark (2007) ‘Analysing and Assessing Accountability: A Conceptual Framework’ *European Law Journal 2007 13:4, 447-468.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1468-0386.2007.00378.x/pdf<. [Accessed 20.08.2014].

Bowers. Mary (2008) ‘Our House, in the Middle of Google's Street’ *The Guardian. 10.04.2008. Webpage.* >http://www.theguardian.com/technology/2008/apr/10/news.google<. [Accessed 12.01.2015].

Bowling. Ben and Amber Marks, Cian Murphy (2008) ‘Crime Control Technologies’ (Ed.) Brownswood. Roger and Karen Yeung. *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*. Hart Publishing. Oxford. United Kingdom.

Bradbury. Danny (2013) ‘How to Manage Cyber-risks Effectively’ *The Guardian 13.02.2013 Webpage.* >http://www.theguardian.com/media-network/media-network-blog/2013/feb/13/manage-cyber-risks-effectively [Accessed 26.07.2014].

Brand. Fridolin S and Kurt Jax (2007) ‘Focusing the Meaning(s) of Resilience: Resilience as a Descriptive Concept and a Boundary Object’ *Ecology and Society 2007 12:1, 23.* >http://www.ecologyandsociety.org/vol12/iss1/art23/<. [Accessed 10.01.2015].

Broadhurst. Roderic (2006) ‘Development in Global Law Enforcement of Cyber-crime’ *Policing, An International Journal of Police Strategies & Management 29:3, 408-433.* >http://www.emeraldinsight.com/journals.htm?articleid=1571786&show=abstract<. [Accessed 09.09.2013].

Brissett. Wilson. N. (2003), ‘Bibliographical Essay on Fear’ *The Hedgehog Review 2003.* >http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved=0CCMQFjAA&url=http%3A%2F%2Fiasc-culture.org%2FTHR%2Farchives%2FFear%2F5.3JBrissett.pdf&ei=OhLKVJ7IIMH67Abp8oCoAw&usg=AFQjCNF7txX4KkiKwj7UiaGoypobEVqURg&sig2=qam2m1J9XjYMKVNA4hiQ7A&bvm=bv.84607526,d.ZGU<. [Accessed 20.12.2014].

Brito. Jerry and Tate Watkins (2011) ‘Loving the Cyber Bomb-The Dangers of Threat Inflation in Cybersecurity Policy’. *3 Harv. Nat'l Security Journal 2011-2012 39:3.* >http://heinonline.org/HOL/LandingPage?handle=hein.journals/harvardnsj3&div=4&id=&page=<. [Accessed 12.12.2014].

Brownswood. Roger (2008) ‘So What does the World Need Now?’ (Ed.) Brownswood. Roger and Karen Yeung. *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*. Hart Publishing. Oxford. United Kingdom.

Brunner. Elgin M. and Myriam Dunn Cavelty (2009) ‘The Formation of In-formation by the US military: Articulation and Enactment of Infomanic Threat Imaginaries on the Immaterial Battlefield of Perception’. *Cambridge Review of International Affairs 2009 2:4, 629-646.* >http://www.tandfonline.com/doi/abs/10.1080/09557570903325454<. [Accessed 20.12.2014].

Bullwinkle. J. (2005) ‘International Cooperation in Combating Cybercrime in Asia: Existing Mechanisms and New Approaches (Ed.) Broadhurst R. and Peter Grabosky (2005) *Cybercrime: The Challenge in Asia*. Hong-Kong University Press. Hong-Kong. China

Burchell. Graham (1991) ‘Peculiar Interests: Civil Society and Governing the System of Natural Liberty’ (Ed.), Burchell. Graham and Colin Gordon, Peter Miller (1991) *The Foucault Effect. Studies in Governmentality.* Hemel Hempstead: Harvester Wheatsheaf. United Kingdom.

Burgess, J. Peter (2007) ‘Social Values and Material Threat: The European Programme for Critical Infrastructure Protection’ *International journal of critical infrastructures* 32007 3:3-4, 471-487. >http://www.inderscienceonline.com/doi/abs/10.1504/IJCIS.2007.014121<. [Accessed 20.05.2015].

Burnett. Jonny and Dave Whyte (2005) ‘Embedded Expertise and the New Terrorism’ *Journal for Crime, Conflict and the Media 1:4, 1-18.* >http://www.diplomatie.gouv.fr/fr/IMG/pdf/expertise_terrorisme.pdf<. [Accessed 04.09.2013].

Burris. Scott and Michael Kempa, Clifford Shearing (2008) ‘Changes in Governance: A Cross-Disciplinary Review of Current Scholarship’ *Akron Law Review 2008 41:1, 1-66.* >http://heinonline.org/HOL/Page?handle=hein.journals/aklr41&div=4&collection=journals&set_as_cursor=0&men_tab=srchresults&terms=30 Bull. Austl. Soc. Leg. Phil 30|30 Austl. J. Leg. Phil. 30&type=matchall<. [Accessed 19.12.2014].

Burris. Scott and Peter Drahos, Clifford Shearing (2005) ‘Nodal Governance’ *Australian Journal of Legal Philosophy 30, 1-43.* >http://papers.ssrn.com/sol3/papers.cfm?abstract_id=760928<. [Accessed 07.09.2013].

BusinessDictonary (2013) ‘Risk. Definition’ *Webpage.* >http://www.businessdictionary.com/definition/risk.html<. [Accessed 20.06.2013].

BusinessDictionary (2014) ‘Cyber theft’ *Webpage.* >http://www.businessdictionary.com/definition/cybertheft.html#ixzz3NI4c7Ih2<. [Accessed 20.06.2013].

Buzan. Barry (1987) *An Introduction to Strategic Studies: Military Technology and International Relations*. Macmillan. London. United Kingdom.

Buzan. Barry (1991a) *People, States and Fear: An Agenda for Security Studies in the Post-Cold War Era*. Lynne Rienner. Boulder. United Kingdom.

Buzan. Barry (1991b) ’Is International Security Possible? (Ed.) Booth. Ken (1992) *New Thinking about Strategy and International Security*. HarperCollins. United Kingdom.

Buzan. Barry and Lene Hansen (2009) *The Evaluation of International Security Studies.* Cambridge University Press. United Kingdom.

Buzan. Barry, Ole Wæver and Jaap de Wilde (1998) *Security. A New Framework for Analysis.* Lynne Rienner Publishers. United Kingdom.

Caballero-Anthony. Mely and Ralf Emmers, Amitav Acharya (2006) *Non-traditional Security in Asia: Dilemmas in Securitization.* Ashgate. London. United Kingdom.

Caldwell. Tracey (2011) ’Ethical Hackers: Putting on the White Hat’ *Network Security 2011 7, 10-13.* >http://www.sciencedirect.com/science/article/pii/S1353485811700757#<. [Accessed 28.08.2014].

Caldwell. Tracey (2013) ‘Risky Business: Why Security Awareness is Crucial for Employees’ *The Guardian. 12.02.2013. Webpage.* >http://www.theguardian.com/media-network/media-network-blog/2013/feb/12/business-cyber-security-risks-employees<. [Accessed 27.07.2014].

Carr. Jeffrey (2012) *Inside Cyber Warfare: Mapping the Cyber Underworld*. O’Reilly, Sebastopol. Canada.

Carrera. Sergio, Marie De Somer and Bilyana Petkova (2012) 'The Court of Justice of the European Union as a Fundamental Rights Tribunal: Challenges for the Effective Delivery of Fundamental Rights in the Area of Freedom, Security and Justice' *CEPS Papers in Liberty and Security in Europe 49.* >http://papers.ssrn.com/sol3/papers.cfm?abstract_id=214589<. [Accessed 19.12.2014].

C.A.S.E. Collective (2006) 'Critical Approaches to Security in Europe: a Networked Manifesto' *Security Dialogue 2006 37:4, 443-487.* >http://sdi.sagepub.com/content/37/4/443.full.pdf+html<. [Accessed 28.08.2013].

CERT-EU (2013) 'About Us' *News Monitor. Webpage.* >http://cert.europa.eu/cert/plainedition/en/cert_about.html<. [Accessed 09.09.2013].

Charmaz. Kathy (2014) *Constructing Grounded Theory*. Sage. London. United Kingdom.

Chulov. Martin (2015) 'Jordanians Turn their Minds to Revenge after Isis Killing of Pilot' *The Guardian. 04.02.2015.* Webpage. >http://www.theguardian.com/world/2015/feb/04/isis-muadh-al-kasasbeh-death-jordan-revenge-mood<. [Accessed 05.02.2015].

Clapperton. Guy (2013) 'Who are the Hackers? Profiling the Masters of Data Disruption' *The Guardian. 11.02.2013. Webpage.* >http://www.theguardian.com/media-network/media-network-blog/2013/feb/11/hackers-hacktivists-cybercriminals-virus-data<. [Accessed 26.07.2014].

Clarke. Richard (1999) 'Threats to US National Security: Proposed Partnership Initiatives towards Preventing Cyber Terrorist Attacks'. *DePaul Bus. LJ 1999 12: 33.>* http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/depbus12&section=6<. [Accessed 20.12.2014].

Clarke. Richard A. and Robert K. Knake (2010) *Cyberwar. The Next Threat to National Security and What to Do About It.* HaperCollins Publisher. New York. United States.

Clauset. Arron and Maxwell Young and Kristian Skrede Gleditsch (2007) 'On the Frequency of Severe Terrorist Events' *Journal of Conflict Resolution 2007 51:1, 58-87.* >http://jcr.sagepub.com/content/51/1/58.full.pdf+html<. [Accessed 27.08.2014].

Coaffee. Jon (2006) 'From Counterterrorism to Resilience' *The European Legacy: Toward New Paradigms 2006 11:4, 389-403.* >http://www.tandfonline.com/doi/full/10.1080/10848770600766094<. [Accessed 09.09.2013].

Coaffee. Jon and Peter Rogers (2008) 'Rebordering the City for new Security Challenges: From Counter-terrorism to Community Resilience' *Space and Polity* 2008 12:1, 101-118. >http://www.tandfonline.com/doi/abs/10.1080/13562570801969556<. [Accessed 29.05.2015].

Coaffee Jon and David Murkami-Wood, Pete Rogers (2008) *The Everyday Resilience of the City* Palgrave/Macmillian, Basingstoke. United Kingdom.

CODEXTER (2007) 'Opinion of the Committee of Experts on Terrorism (CODEXTER) for the Attention of the Committee of Ministers on Cyberterrorism and Use of Internet for Terrorist Purposes' *CoE, Webpage.* >http://www.coe.int/t/dlapil/codexter/cyberterrorism_en.asp<. [20.07.2014].

Cohn. Carol (2011) '"Feminist Security Studies": Toward a Reflexive Practice' *Politics & Gender 2011 7:4, 581-586.* >http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=8491408&fileId=S1743923X11000389<. [Accessed 20.12.2014].

Coker. Christopher (2002) 'Globalisation and Insecurity in the Twenty-first Century: NATO and the Management of Risk' *Adelphi Paper 345*. Oxford University Press. United Kingdom.

Collins. Alan (2010) 'Introduction: What is Security Studies' (Ed.) Collins. Alan. *Contemporary Security Studies.* Oxford University Press, Oxford. United Kingdom.

Collins. John (2000) **'**Preemptive Prevention' *Journal of* Philosophy *2000 97:4, 223-234.* >http://www.jstor.org/stable/pdfplus/2678391.pdf< . [Accessed 05.09.2013].

Connolly. Kate (2013) 'Angela Merkel: NSA Snooping claims 'Extremely Serious' *The Guardian. 03.07.2013. Webpage.* >http://www.theguardian.com/world/2013/jul/03/angela-merkel-nsa-snooping-serious<. [Accessed 21.07.2014].

Conrad. James (2012) 'Seeking Help: The Important Role of Ethical Hackers' *Network Security 2012 8, 5-8.* >http://www.sciencedirect.com/science/article/pii/S1353485812700715<. [Accessed 28.08.2014].

Conteh-Morgan. Earl (2005) 'Peacebuilding and Human Security: A Constructivist Perspective' *International Journal of Peace Studies 2005 10:1, 69-86.* >http://scholar.google.co.uk/scholar?q=Conteh-

Morgan,+E.+(2005)+%E2%80%98Peacebuilding+and+human+security:+a+constructivist+perspective%E2%80%99&hl=en&as_sdt=0&as_vis=1&oi=scholart&sa=X&ei=hGvHVN_0KMSzUdS3gZgC&ved=0CCAQgQMwAA<. [Accessed 18.12.2014].

Continuity Central (2011) 'Cooperative Models for Effective Public Private Partnerships' *The International Business Continuity Information Portal. 11.10.2011.* >http://www.continuitycentral.com/news05973.html <. [Accessed 06.09.2013].

Cooper. Melinda (2006) 'Pre-empting Emergence: the Biological Turn in the War on Terror' *Theory, Culture and Society 2006 23:4, 113–35.* >http://webcache.googleusercontent.com/search?q=cache:RYWcQsR_5RsJ:www.16beavergroup.org/drift/readings/pre-empting-emergence.pdf+&cd=1&hl=en&ct=clnk&gl=uk<. [Accessed 20.12.2014].

Corbin. Juliet and Anslem Strauss (1990). *Basics of Grounded Theory Methods*. Sage. Beverly Hills. United States.

Corbin. Juliet and Anselm Strauss (2014) *Basics of qualitative research: Techniques and procedures for developing grounded theory.* Sage publications. Thousand Oaks. United States.

Corbin. Juliet and Anslem Strauss (1990) 'Grounded theory research: Procedures, canons, and evaluative criteria', Qualitative sociology 1990 13:1, 3-21. >http://link.springer.com/article/10.1007/BF00988593#page-1<. [Accessed 25.05.2015].

Corry. Olaf (2010) 'Securitization and 'Riskiziation': Two Grammars of Security' *Working Paper. 7th Pan-European International Relations Conference, Stockholm 9th-11th September.* >http://www.stockholm.sgir.eu/uploads/Risk%20society%20and%20securitization%20theory%20SGIR%20paper.pdf<. [Accessed 05.09.2013].

Cottey. Andrew (2007) *Security in the New Europe*. Palgrave MacMillan. Hampshire and New York.

Council of Europe (1950) *The European Convention on Human Rights.* >http://www.echr.coe.int/Documents/Convention_ENG.pdf<. [Accessed 09.09.2013].

Council of Europe (2001) *Convention on Cybercrime*. *ETS No. 185.* >http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm<. [Accessed 06.09.2013].

Council of Europe (2005) *Convention on the Prevention of Terrorism*. >http://conventions.coe.int/Treaty/en/Treaties/Html/196.htm<. [Accessed 06.09.2013].

Council of Europe (2007a) 'How to Prevent Cybercrime against State Institutions in Member and Observer States? *Parliamentary Resolution 1565 (2007)* >http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta07/eres1565.htm<. [Accessed 27.05.2014].

Council of Europe (2007b) 'A Political Framework for Co-operation against Cyber-attacks. Motion for Recommendation. Presented by Mrs. Ojuland and Other' *Document 11349. Parliamentary Assembly.* >http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=11695&Language=EN<. [Accessed 09.09.2013].

Council of Europe (2013b) 'Who We Are' *Webpage.* >http://www.coe.int/aboutCoe/index.asp?page=nosObjectifs&l=en#<. [Accessed 06.09.2013].

Council of Europe (2014a) 'Action for Terrorism' *Webpage.* >http://www.coe.int/t/dlapil/codexter/cyberterrorism_en.asp<. [Accessed 18.07.2014]

Council of Europe (2014b) 'Cyber-crime. A Threat to Democracy, Human Rights and the Rule of Law' *The Council in Brief. Webpage.* >http://hub.coe.int/web/coe-portal/what-we-do/rule-of-law/cybercrime?dynLink=true&layoutId=36&dlgroupId=10226&fromArticleId=<. [Accessed 23.04.2014].

Council of Europe (2014d) 'The Council of Europe and the Internet. Freedom and Safety Online' *Internet Governance. Webpage.* >http://hub.coe.int/en/a-free-and-safe-internet/<. [Accessed 23.04.2014].

Council of Europe (2015) 'The Council of Europe's Convention on Cybercrime' *Chart of Signatures and Ratifications CERTs No: 185. Webpage.* >http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG<. [Accessed 09.09.2013].

Council of the European Union (2003) 'Council Resolution on a European Approach towards a Culture of Network and Information Security' *TELECOM 78, JAI 307, PESC*

593. >http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.oecd.org%2Fsti%2Fieconomy%2Feures.pdf&ei=Q3nJVLP0GZOP7AaV3oGoAg&usg=AFQjCNG84yhu0KifiUZ6XaUArX2fT1zysA&sig2=btN_vGdo_lb_PeO_BnzFrw&bvm=bv.84607526,d.ZGU<.[Accessed 20.12.2014].

Coward. Martin (2012) 'Between us in the city: Materiality, Subjectivity, and Community in the Era of Global Urbanization' *Environment and Planning D: Society and Space* 2012 30:3, 468-481. >http://www.envplan.com/openaccess/d21010.pdf<. [Accessed 30.05.2015].

Craig. Paul (2010) *The Lisbon Treaty. Law, Politics, and Treaty Reform*. Oxford University Press. Oxford. United Kingdom.

Craig. Paul and Gráinne de Búrca (2008) *EU Law, Text, Cases and Materials*. Oxford University Press. Oxford. The United Kingdom.

Crawford. Andrew (2003) ''Contractual Governance' of Deviant Behaviour' *Journal of Law and Society 2003 30:4, 479-505.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1467-6478.2003.00267.x/pdf<. [Accessed 06.09.2013].

Crawford. Andrew (2006) 'Networked Governance and the Post-regulatory State? Steering, Rowing and Anchoring the Provision of Policing and Security' *Theoretical Criminology 2006 10:4, 449-479.* >http://tcr.sagepub.com/content/10/4/449.full.pdf<. [Accessed 06.09.2013].

Crawford. Andrew and Stuart Lister (2004) *The Extended Policing Family: Visible Patrols in Residential Areas*. Joseph Rowntree Foundation. York. United Kingdom.

Cresci. Elena (2014) 'How to Get Around Turkey's Twitter Ban' *The Guardian. 21.03.2014. Webpage.* >http://www.theguardian.com/world/2014/mar/21/how-to-get-around-turkeys-twitter-ban<. [Accessed 22.04.2014].

Creswell. John (2007) 'Review of the Literature', *Research Design: Qualitative, Quantitative, and Mixed Method Approaches.* Sage Publications. London. United Kingdom.

Christie. Daniel J. (2011) *The Encyclopedia of Peace Psychology*. Blackwell. United Kingdom.

Dale. Roger (2004) 'Governance, Governmentality and the OMG' (Ed.) Larner. Wendy. And William Walters. *Global Governmentality. Governing International Spaces*. Routledge. Abingdon. United Kingdom.

Dam. Kenneth W. and Herbert S. Lin (1996) *Cryptography's Role in Securing the Information Society. Committee to Study National Cryptography Policy, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council*. The National Academic Press. Washington, DC. United States.

Dasse. Christopher and Oliver Kessler (2007) 'Known and Unknowns in the 'War on Terror': Uncertainty and the Political Construction of Danger' *Security Dialogue 38: 4, 411–434.* >http://sdi.sagepub.com/content/38/4/411.short<. [Accessed 27.08.2014].

Dean. Mitchell (1994) *Critical and Effective Histories: Foucault's Methods and Historical Sociology*. Routledge. London. United Kingdom.

Dean. Mitchell (1999) 'Risk, Calculable and Incalculable' (Ed.) Lupton. Deborah. *Risk and Sociocultural Theory. New Directions and Perspectives.* Cambridge University Press. Cambridge. United Kingdom.

Dean. Mitchell (2002) 'Powers of Life and Death beyond Governmentality' *Cultural Values 2002 6:1-2, 119-138.* >http://www.tandfonline.com/doi/abs/10.1080/1362517022019775<. [Accessed 12.01.2015].

Dean. Mitchell (2010) Governmentality. Power and Rule in Modern Society. Sage. London. United Kingdom

De Goede. Marieke (2008a) 'Beyond Risk: Premediation and the Post-9/11 Security Imagination' *Security Dialogue 2008 39:2-3,155-176.* >http://sdi.sagepub.com/content/39/2-3/155.short<. [Accessed 19.12.2014].

De Goede. Marieke (2008b) 'The Politics of Preemption and the War on Terror in Europe' *European Journal of International Relations 2008 14:1, 161-186.* >http://ejt.sagepub.com/content/14/1/161.full.pdf<. [Accessed 06.09.2013].

De Goede. Marieke. and Samuel Randalls (2009) **'**Precaution, Preemption: Arts and Technologies of the Actionable Future' *Environment and Planning Development: Society and Space 2009 27:5, 859-878.* >http://www.envplan.com/epd/fulltext/d27/d2608.pdf<. [Accessed 09.09.2013].

Deibert. Ronald (2002) ‘Circuits of Power: Security in the Internet Environment’ (Ed.) Rosenau James N. and J. P. Singh (2002) *Information Technologies and Global Politics: The Changing Scope of Power and Governance*. University of New York. Albany. United States.

Deibert. Ronald J. and Masashi Crete-Nishihata (2013) ‘Global Governance and the Spread of Cyberspace Controls’ *Global Governance: A Review of Multilateralism and International Organizations 2013 18:3, 339-361.* >http://journals.rienner.com/doi/abs/10.5555/1075-2846-18.3.339<. [Accessed 18.12.2014].

Deibert. Ronald J. and Rafal Rohozinski. (2008) ‘Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet’ (Ed.) Ronald J. Deibert and John Palfrey, Rafal Rohozinski, Jonathan Zittrain (2008) *Access Denied: The Practice and Policy of Global Internet Filtering*. MIT Press Cambridge, United States.

Deibert. Ronald, and Rafal Rohozinski (2010a) ‘Liberation vs. Control: The Future of Cyberspace’ *Journal of Democracy 2010 21:4, 43-57.* > http://onlinelibrary.wiley.com/doi/10.1111/j.1749-5687.2009.00088.x/full<. [Accessed 18.12.2014].

Deibert. Ronald J. and Rafal Rohozinski (2010b) ‘Risking Security: Policies and Paradoxes of Cyberspace Security’ *International Political Sociology 2010 4, 15-32.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1749-5687.2009.00088.x/pdf<. [Accessed 09.09.2013].

Denning. Dorothy (1999) *Information Warfare and Security*. Addison-Wesley. New York. United States.

Denning. Dorothy (2000) ‘Cyberterrorism, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services’ *US House of Representatives, 23.05.2000.* >http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf<. [Accessed 09.09.2013].

Denning. Dorothy (2006) ‘A View of Cyberterrorism Five Years Later’ (Ed.) Himma. Kenneth (2006) *Readings in Internet Security: Hacking, Counterhacking, and Society.* Jones and Bartlett Publishers, Boston, United States. >http://faculty.nps.edu/dedennin/publications/Cyberterror%202006.pdf<. [Accessed 20.01.2015].

Denning. Dorothy E. (2010) ‘Terror's Web: How the Internet is Transforming Terrorism’ (Ed.) Jewkes. Y. and Majid Yar (2010) *Handbook on Internet Crime*. Willan Publishing.>http://faculty.nps.edu/dedennin/publications/Denning-TerrorsWeb.pdf<. [Accessed 15.12.2014].

Denning. Dorothy. E. (2012) ‘Stuxnet: What Has Changed?’ *Future Internet 2012, 4, 672-687.* >http://faculty.nps.edu/dedennin/publications/Stuxnet%20-%20What%20Has%20Changed%20-%20Future%20Internet%20-%20final.pdf<. [Accessed 12.12.2014].

Der Derian. James (2005) ‘Imaging Terror: Logos, Pathos and Ethos’ *Third World Quarterly .The Politics of Naming: Rebels, Terrorists, Criminals, Bandits and Subversives 2005 26:1, 23-37.* >http://www.jstor.org/stable/3993761?seq=1#page_scan_tab_contents<. [Accessed 12.12.2014].

Dershowitz. Alan M. (2006) *Preemption: A Knife That Cuts Both Ways*. W. W. Norton. New York. United States.

Dipert. Randall R. (2010) ‘The Ethics of Cyberwarfare’ *Journal of Military Ethics 2010 9: 4, 384-410.* >http://www.tandfonline.com/doi/pdf/10.1080/15027570.2010.536404<. [Accessed 06.09.2013].

Dorgan. Byron (2013) ‘Cyber Terror Is the New Language of War’ *Huffington Post. Politics. The Blog. 17.07.2013. Webpage.* >http://www.huffingtonpost.com/sen-byron-dorgan/cyber-terror-is-the-new-l_b_3612888.html<. [Accessed 18.07.2014].

Douglas-Scott. Sionaidh (2011) ‘The European Union and Human Rights after the Treaty of Lisbon’ *Human Rights Law Review, 1:4, 645-682.* >http://hrlr.oxfordjournals.org/content/11/4/645.short<. [Accessed 19.12.2014].

Douglas. Mary (1986) *Risk Acceptability According to Social Science*. Routledge. London. United Kingdom

Douglas. Mary (1990) ‘Risk as a Forensic Resource’ *Daedalus 1990 119:4, 1-16.* >http://www.jstor.org/stable/pdfplus/20025335.pdf?acceptTC=true<. [Accessed 06.09.2013].

Dowdle. Michael (2006) *Public Accountability: Designs, Dilemmas and Experiences*. Cambridge University Press. Cambridge. United Kingdom.

Dunn Cavelty. Myriam (2007) *Cyber-security and Threat Politics: US Efforts to Secure the Information Age.* Routledge, Abingdon. United Kingdom.

Dunn Cavelty. Myriam (2008) ‘Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate’ *Journal of Information Technology & Politics 2008 4:1,19-36.* >http://www.tandfonline.com/doi/abs/10.1300/J516v04n01_03<. [Accessed 19.12.2014].

Dunn Cavelty. Myriam (2013) ‘From Cyber-bombs to Political Fallout: Threat Representation with an Impact in the Cyber-security Discourse’ *International Studies Review, 2012 15:1.* >http://ssrn.com/abstract=2200862<. [Accessed 21.12.2014].

Dunn Cavelty. Myriam, and Kristian S. Kristensen (2008) ‘{Securing\'the homeland\': Critical Infrastructure, Risk and (In)Security’. >http://www.citeulike.org/group/17991/article/12364908<. [Accessed 20.12.2014].

Dunn Cavelty. Myriam and Victor Mauer (2009) ‘Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence’ *Security Dialogue 2009 40:2, 123-144.* >http://sdi.sagepub.com/content/40/2/123.full.pdf<. [Accessed 08.09.2013].

Dunn Cavelty. Myriam and Manuel Suter (2009) ‘Private-Public Partnerships are no Silver-Bullet: an Expanded Governance Model for Critical Infrastructure Protection’ *International Journal of Critical Infrastructure Protection 2009 2:4, 179-187.* >http://www.sciencedirect.com/science/article/pii/S1874548209000274<. [Accessed 12.09.2013].

Durodié. Bill (2004) ‘The Limitations of Risk Management: Dealing with Disasters and Building Social Resilience’. *Tidsskriftet Politik* 2004 8:1, 14-21. >http://www.durodie.net/index.php/site/article/50/<. [Accessed 28.05.2015].

Cavelty. Myriam Dunn and Mareile Kaufmann, Kristian Søby Kristensen (2015) ‘Resilience and (in) Security: Practices, Subjects, Temporalities’ *Security Dialogue* 2015 46:1, 3-14. >http://sdi.sagepub.com/content/46/1/3.short<. [Accessed 27.05.2015].

Dupont. Benoît (2006) ‘Power Struggles in the Field of Security: Implications for Democratic Transformation’ (Ed.) Wood. Jennifer and Benoît Dupont (2006) *Democracy, Society and the Governance of Security.* Cambridge University Press. Cambridge. United Kingdom.

Dupont. Benoît. and Peter Grabosky, Clifford Shearing (2003) ‘The Governance of Security in Weak and Failing States’ *Criminal Justice 3, 331-346.* >http://crj.sagepub.com/content/3/4/331.full.pdf+html<. [Accessed 19.12.2014].

Eijkman. Quirine (2012) ‘Counter-Terrorism, Technology and Transparency: Reconsidering State Accountability?’ *ICCT International Centre for Counter-Terrorism - The Hague. Discussion Paper.* > https://www.counterextremism.org/resources/details/id/300/counter-terrorism-technology-and-transparency-reconsidering-state-accountability<. [Accessed 10.12.2014].

Ellison. Louise (2001) ‘Cyber Stalking. Tackling Harassment on the Internet’ (Ed.) Wall. David S. (2001) *Crime and the Internet.* Routledge. Abingdon. United Kingdom.

Embar-Seddon. Ayn (2002) ‘Cyberterrorism: Are We under Siege?’ *American Behavioural Scientist 2002 45: 6, 1033*-1043. >http://abs.sagepub.com/content/45/6/1033.full.pdf+html<. [Accessed 06.09.2013].

Emmers. Ralf (2010) ’Securitization’ (Ed.) Collins. Alan. *Contemporary Security Studies.* Oxford University Press. Oxford. United Kingdom.

Ericson. Richard V. (2007a) ’Rules in Policing: Five Perspectives’ *Theoretical Criminology 2007 11:3, 367–401.* >http://tcr.sagepub.com/content/11/3/367.full.pdf<. [Accessed 04.09.2013].

Ericson. Richard V. (2007b) ’Security, Surveillance and Counter-law’ *Criminal Justice Matters 2007 68: 1, 6-7.* >http://www.tandfonline.com/doi/pdf/10.1080/09627250708553271<. [Accessed 04.09.2013].

Ericson. Richard V. (2008) ’The State of Pre-emption’ (Ed.) Amoore. Louise and Marieke de Goede. *Risk and the War on Terror.* Routledge. Abingdon. The United Kingdom.

Ericson. Richard V. and Aaron Doyle (2004) ‘Catastrophe Risk, Insurance and Terrorism’ *Economy and Society 2004 33:2, 135–173.* >http://www.tandfonline.com/doi/pdf/10.1080/0308514041000l677102<. [Accessed 03.09.2013].

Erikson. Kai (1994) *A New Species of Trouble: Explorations in Disaster, Trauma, and Community*. London: W.W Norton and Co.

EUROPA (2015) ‘European region’ *Web-page.* >Europe_subregion_map_UN_geoschme.svg. http://europa.eu/about-eu/countries/index_en.htm<. [Accessed 10.02.2015].

EUROPA (2015) ‘EU Countries‘ *Web-page*. >http://europa.eu/about-eu/countries/index_en.htm<. [Accessed 10.02.2015].

EURACTIV (2011) ‘Cyber-attacks Now the most Feared EU Energy Threat’ *Energy News*. *Webpage.* >http://www.euractiv.com/energy/cyber-attacks-feared-eu-energy-t-news-501547<. [Accessed 12.09.2013].

EURACTIV (2012) ‘European Renewable Power Grid Rocked by Cyber-attack’ *Energy Supply*. *Webpage.* >http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541<. [Accessed 10.09.2013].

Eurojust (2011) *Eurojust Annual Report 2011*. >http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202011/Annual-Report-2011-EN.pdf<. [Accessed 09.09.2013].

European Commission (2004) ‘Critical Infrastructure Protection in the Fight against Terrorism’ *Communication from the Commission to the Council and the European Parliament COM(2004) 702 final*. >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF<. [Accessed 08.09.2013].

European Commission (2006a) ‘A European Programme for Critical Infrastructure Protection’ *Communication from the Commission COM(2006) 786 final.* >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF<. [Accessed 08.09.2013].

European Commission (2006b) ‘A strategy for a Secure Information Society – Dialogue, Partnership and Empowerment’ *COM(2006) 251 final’.* >http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52006DC0251<. [Accessed 20.08.2014].

European Commission (2007a) ‘Green Paper on Bio-Preparedness’ *Commission of the European Communities COM(2007) 399 final.* >http://ec.europa.eu/food/resources/gp_bio_preparedness_en.pdf<. [Accessed 03.09.2013].

European Commission (2007b) ‘Towards a General Policy on the Fight against Cyber *Crime’ Commission of the European Communities. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions COM(2007) 267 final*. >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF<. [Accessed 12.09.2013].

European Commission (2008) ‘Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against Information Systems’ *Report from the Commission to the Council COM (2008) 448 final*. >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0448:FIN:EN:PDF<. [Accessed 12.09.2013].

European Commission (2009a) ‘Commission Acts to Protect Europe from Cyber-attacks and Disruptions’ *Press Release IP/09/494. Webpage.* >http://europa.eu/rapid/press-release_IP-09-494_en.htm<. [Accessed 12.09.2013].

European Commission (2009b) ’Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience’ *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 COM(2009) 149 final.* >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF<. [Accessed 09.09.2013].

European Commission (2009c) ‘Protecting Europa from Large Scale Cyber-attacks and Disruption’ *Summaries of EU Legislation. Web-page.* >http://europa.eu/legislation_summaries/information_society/internet/si0010_en.htm<. [Accessed 09.09.2013].

European Commission (2010a) ‘Attacks against Information Systems and Repealing Council Framework Decision 2005/222/JHA’ *Proposal for a Directive of the European Parliament and of the Council COM (2010) 517 final.* >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF<. [Accessed 09.09.2013].

European Commission (2010b) ‘A Digital Agenda for Europe’ *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM (2010) 245 final/2*. >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=com:2010:0245:fin:en:pdf<. [Accessed 12.09.2013].

European Commission (2010c) ‘Commission to Boost Europe's Defences against Cyber-attacks’ *Press Release. Webpage.* >http://europa.eu/rapid/press-release_IP-10-1239_en.htm<. [Accessed 09.09.2013].

European Commission (2010d) ‘Cyber Security: EU and US strengthen Transatlantic Cooperation in Face of mounting Global Cyber-security and Cyber-crime Threats’ *Press Release MEMO 11/24.* Webpage. >http://europa.eu/rapid/press-release_MEMO-11-246_en.htm<. [Accessed 10.09.2013].

European Commission (2010e) ‘Delivering an Area of Freedom, Security and Justice for Europe's Citizens Action Plan Implementing the Stockholm Programme’ *European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2010) 171 final*. >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF<. [Accessed 06.09.2013].

European Commission (2010f) *Internal Security Strategy for the European Union: ”Towards a European Security Model.* >http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf<. [Accessed 12.09.2013].

European Commission (2010g) ‘Joint Statement of the EU-U.S. Summit – 20 November 2010 – Lisbon’ *Press Release MEMO10/597. Webpage.* >http://europa.eu/rapid/press-release_MEMO-10-597_en.htm<. [Accessed 10.08.2013].

European Commission (2010h) ‘Non-Paper on the Establishment of a European Public-Private Partnership for Resilience (EP3R)’ *2010. Version 2.0 – 23 June 2010.* >http://cesedenciber.wikispaces.com/file/view/2010_06_23_ep3r_nonpaper_v_2_0_final.pdf<. [Accessed 08.09.2013].

European Commission (2010i) ‘The EU Internal Security Strategy in Action: Five Steps towards a More Secure Europe’ *Communication from the Commission to the European Parliament and the Council COM(2010) 673 final.* >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF<. [Accessed 08.09.2013].

European Commission (2010j) ‘The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens’ *Official Journal of the European Union. Notice from the European Institutions, Bodies, Offices and Agencies. European Council 2010/C 115/01.* >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF<. [Accessed 07.09.2013].

European Commission (2010k) **‘**Proposal for a Directive on Attacks against Information Systems, Repealing Framework Decision 2005/222/JHA’. *Press Release. Memo/10/463*. > http://europa.eu/rapid/press-release_MEMO-10-463_en.htm<.

European Commission (2011a) ‘Achievements and the Next Steps: Towards Global Cyber-Security’ *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Central Information Infrastructure Protection COM (2011) 163 final.* >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF<. [Accessed 09.09.2013].

European Commission (2011b) ‘European Principles and Guidelines for Internet Resilience and Stability’ *Version of March 2011.* >http://ec.europa.eu/danmark/documents/alle_emner/videnskabelig/110401_rapport_cyberangreb_en.pdf<. [Accessed 12.09.2013].

European Commission (2012a) ‘Special Eurobarometer 390. Cyber Security’ *Fieldwork: March 2012. Publication: July 2012.* >http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf<. [Accessed 09.09.2013].

European Commission (2012b) ‘Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre’ *Communication from the Commission to the Council and the European Parliament COM(2012) 140 final.* >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF<. [Accessed 05.09.2013].

European Commission (2013a) ‘Action 32: Strengthen the Fight against Cybercrime and Cyber-attacks at International Levels’ *The Digital Agenda. Webpage.* >http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-32-strengthen-fight-against-cybercrime-and-cyber-attacks<. [Accessed 09.09.2013].

European Commission (2013b) ‘Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection’ *23.12.2008. L 345/75.* >http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008L0114<. [Accessed 20.12.2014].

European Commission (2013c) ‘International Digital Agenda Policy: Internet Governance, Internet Security, Market Access. *The Digital Agenda. About International. Webpage.* >http://ec.europa.eu/digital-agenda/en/about-international<. [Accessed 12.09.2013].

European Commission (2013d) ‘Measures to Ensure a High Common Level of Network and Information Security Across the Union’ *Proposal for a Directive of the European Parliament and the Council COM(2013) 48 final.* >http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf<. [Accessed 09.09.2013].

European Commission (2013e) ‘NIS Public-Private Platform – Call for Expression of Interest’ *Press Release. Webpage.* >http://ec.europa.eu/digital-agenda/en/news/nis-public-private-platform-—-call-expression-interest<. [Accessed 09.09.2013].

European Commission (2013h) ‘Proposed Directive on Network and Information Security – Frequently Asked Questions’ *MEMO/13/71. Press Release. Webpage.* >http://europa.eu/rapid/press-release_MEMO-13-71_en.htm< [Accessed 09.09.2013].

European Commission (2013i) Proposal Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union. COM (2013) 48 Final. 2013/0027(COD). >http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0048<. [Accessed 05.02.2014].

European Commission (2014a) ‘Cybercrime’. *What we Do Webpage.* >http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm<. [Accessed 05.02.2014].

European Commission (2014b) ‘Flagship Initiatives’ *Europe 2020 Strategy.* > http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_en.htm<. [Accessed 01.09.2014].

European Commission (2014c) ‘Proposal for a Directive on Attacks against Information Systems, Repealing Framework Decision 2005/222/JHA’ *Press release. MEMO/10/463. Webpage.* > http://europa.eu/rapid/press-release_MEMO-10-463_en.htm<. [Accessed 21.07.2014].

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013) ‘Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’ *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions JOIN (2013) final 1.* >http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf<. [Accessed 08.09.2013].

European Council (2005) Council Decision Framework on Attacks against Information Systems *2002/0086 (CNS).* >http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52002PC0173<. [Accessed 01.12.2014].

European Cybercrime Centre (2014a) ‘A Collective Response to Cybercrime’ *Europol. Webpage.* >https://www.europol.europa.eu/ec3<. [Accessed 20.08.2014].

European Cybercrime Centre (2014b) ’Joining Forces to Catch the Criminals’ *Europol Webpage.* >https://www.europol.europa.eu/ec3/joining-forces<. [Accessed 23.07.2014].

European Network Information and Security Agency (2011) ‘Cyber Atlantic’ *ENISA. Webpage.* >http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic/cyber-atlantic-2011<. [Accessed 06.05. 2013].

European Network and Information Security Agency (2013a) ‘ENISA Lists Top Cyber-threats in this Year’s Threat Landscape Report’ *Press Release. Webpage.* >http://www.enisa.europa.eu/media/press-releases/enisa-lists-top-cyber-threats-in-this-year2019s-threat-landscape-report<. [Accessed 26.07.2014].

European Network and Information Security Agency (2013b) ‘FAQ on ENISA and ENISAS’ *European Information Sharing and Alert System.* Webpage. >http://www.enisa.europa.eu/media/faq-on-enisa/faq-on-enisa-and-eisas<. [Accessed 09.09.2013].

European Network and Information Security Agency (2014a) ‘Biggest EU Cyber Security Exercise to Date: Cyber Europe 2014 Taking Place Today’ *Press Release. 28.04.2014. Webpage.* >http://www.enisa.europa.eu/media/press-releases/biggest-eu-cyber-security-exercise-to-date-cyber-europe-2014-taking-place-today<. [Accessed 23.07.2014].

European Network and Information Security Agency (2014b) ‘European Public-Private Partnership for Resilience (EP3R)’ *ENISA. Webpage.* >http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r<. [Accessed 08.0.2013].

European Network and Information Security Agency (2014c) 'News on National Cyber Security Strategies in the European Union and Worldwide' *Webpage.* >http://www.enisa.europa.eu/media/news-items/news-on-national-cyber-security-strategies-in-european-union-and-worldwide<. [Accessed 10.07.2014].

European Public-Private Partnership for Resilience. Working Group 1 (2011a) 'Area 1. Key Assets/ Resources/ Functions for the Continuous and Secure Provisioning of Electronic Communications across Countries' *V3.0 – 02 March 2011. Thematic Sheet*. >http://www.future-internet.eu/uploads/media/EP3R-ToR-Area1-V2.0.pdf<. [Accessed 12.09.2013].

European Public-Private Partnership for Resilience. Working Group 2 (2011b) 'Area 2. Baseline Requirements for Security and Resilience of Electronic Communications' *V3.0 – 03 March 2011. Thematic Sheet*. >http://www.future-internet.eu/uploads/media/EP3R-ToR-Area2-V2.0.pdf<. [Accessed 12.09.2013].

European Public-Private Partnership for Resilience. Working Group 3 (2011c) 'Area 3. Coordination and Cooperation needs and Mechanisms to Prevent and Respond to Large Scale Disruptions Affecting Electronic Communications' *V3.0 – 02 March 2011. Thematic Sheet.* >http://www.future-internet.eu/uploads/media/EP3R-ToR-Area3-V2.0.pdf<. [Accessed 12.09.2013].

European Public-Private Partnership for Resilience (2013a) *Activity Report 2012*. >https://resilience.enisa.europa.eu/ep3r/EP3R-2012-activity-report<. [Accessed 09.09.2013].

European Public-Private Partnership for Resilience (2013b) *Work Objectives*. >https://resilience.enisa.europa.eu/ep3r/ep3r-2013-work-objectives<. [Accessed 09.09.2013].

European Public-Private Partnership for Resilience (2013c) 'Position Paper of the EP3R Task Forces on Incident Management and Mutual Aid Strategies (TF-MASIM)*'* *ENISA. Webpage.* >http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-masim< [Accessed 23.07.2014].

European Public-Private Partnership for Resilience (2013d) 'Position Paper of the EP3R Task Forces on Trusted Information Sharing (TF-TIS)' *ENISA. Webpage.* >http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-tis<. [Accessed 23.07.2014].

European Public-Private Partnership for Resilience (2013e) 'EP3R 2013 – Task Forces on Terminology Definitions and Categorisation of Assets (TF-TDCA)' *ENISA. Webpage.* >http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-tdca<. [Accessed 23.07.2014]

European Union (2002) Council Framework Decision of 13 June 2002 on Combating Terrorism (2002/475/JHA). *22.6.2002. L 164/3Framework Decision on Combating Terrorism.* >http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002F0475<. [Accessed 20.05.2014].

European Union (2003) *A Secure Europe in a Better World. European Security Strategy.* >http://consilium.europa.eu/uedocs/cmsUpload/78367.pdf<. [Accessed 03.09.2013].

European Union (2005) 'Attack against Information Systems' *Official Journal of the European Union. Council Framework Decision 2005/222/JHA. L 69/67.* >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF<. [Accessed 09.09.2013].

European Union (2007) 'Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community' *Official Journal of the European Union 2007/C 306/01.* >http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:FULL:EN:PDF<. [Accessed 09.09.2013].

European Union (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' *L 218/8 Official Journal of the European Union*. >http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32013L0040<.

The European Union (2014) 'Search' *Webpage.* >http://europa.eu/geninfo/query/resultaction.jsp?SMODE=2&ResultCount=10&Collection=EuropaFull&Collection=EuropaSL&Collection=EuropaPR&ResultMaxDocs=200&qtype=simple&DefaultLG=en&ResultTemplate=%2Fresult_en.jsp&page=1&QueryText=cyber+terrorism<. [Accessed 18.07.2014].

Europol (2011a) 'Organised Crime and Trend Assessment' *OCTA 2011.* >https://www.europol.europa.eu/sites/default/files/publications/octa2011.pdf<. [Accessed 09.09.2013].

Europol (2011b) 'TE-SAT 2012. EU Terrorism Situation and Trend Report'. *Corporate publications.* >https://www.europol.europa.eu/content/publication/te-sat-2012-eu-terrorism-situation-and-trend-report-1569<.

Europol (2011c) 'Threat Assessment (Abridged). Internet Facilitated Organised Crime. IOCTA' *Europol Public Information. FILE NO.: 2530-264.* >https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf< [Accessed 09.09.2013).

Europol (2013a) 'Cybercrime: a Growing Global Problem' *Cybercrime Centre (EC3). Webpage.* >https://www.europol.europa.eu/ec3old<. [Accessed 09.09.2013].

Europol (2013b) 'EU Agencies' *Partners. Webpage.* >https://www.europol.europa.eu/content/page/eu-agencies-135<. [Accessed 09.09.2013].

Europol (2013c) 'External Partners' *Partners. Webpage.* >https://www.europol.europa.eu/content/page/external-cooperation-31<. [Accessed 09.09.2013].

Europol (2013d) 'Joining Forces to Catch the Criminals' *The European Cybercrime Centre. Webpage.* >https://www.europol.europa.eu/ec3/joining-forces<. [Accessed 10.09.2013].

Europol (2014a) 'About Us' *Webpage.* >https://www.europol.europa.eu/content/page/about-us<. [Accessed 18.07.2014].

Europol (2014b) 'Europol and Microsoft Enters into New Global Partnerships in Fight against Cybercrime. *Webpage.* >https://www.europol.europa.eu/latest_news/europol-and-microsoft-enters-new-global-partnerships-fight-against-cybercrime<. [Accessed 12.07.2014].

Evans. Brad, and Julian Reid (2013) 'Dangerously Exposed: The Life and Death of the Resilient Subject' Resilience 2013 1:2, 83-98. >http://www.tandfonline.com/doi/abs/10.1080/21693293.2013.770703<. [Accessed 29.05.2015].

Everett. Catherine (2009) 'Ethics – a Question of Right or Wrong'. *Computer Fraud & Security 2009 2, 11-13.* >http://www.sciencedirect.com/science/article/pii/S136137230970020X<. [Accessed 28.08.2014].

Fagan. Kevin (2001) 'The Next Wave of Terror. Scenario Planners Trying to Predict the Unthinkable' *San Francisco Chronicle, 28.10.2001. Webpage.* >http://www.sfgate.com/news/article/The-next-wave-of-terror-Scenario-planners-2865787.php<. [Accessed 10/10/2014].

Feng. Bree (2015) 'Among Snowden Leaks, Details of Chinese Cyberespionage' *The New York Times. 20.01.2015. Webpage.* >http://sinosphere.blogs.nytimes.com/2015/01/20/among-snowden-leaks-details-of-chinese-cyberespionage/?_r=0<. [Accessed 21.01.2015].

Fertik. Michael (2014) 'The 'Right to be Forgotten' may Help Protect our Digital Dignity' *The Guardian, Technology. Commentary, Webpage.* >http://www.theguardian.com/media-network/media-network-blog/2014/jul/11/right-forgotten-google-eu-law#start-of-comments<. [Accessed 15.07.2014].

Fierke. Karin M. (2007) 'Constructivism' (Ed.) Dunne. Tim and Milja Kurki, Steve Smith (2007) *International Relations Theories. Discipline and Diversity.* Oxford University Press. Oxford. United Kingdom.

Fisher. Elizabeth (2001) 'Is the Precautionary Principle Justifiable?' *Journal of Environmental Law 2001 13:3, 315-334.* >http://jel.oxfordjournals.org/content/13/3/315.full.pdf<. [Accessed 08.09.2013].

Fitzpatrick. Joan (2003) 'Speaking Law to Power: The War against Terrorism and Human Rights' *European Journal of International* Law 2003 14: 2, 241-264. >http://ejil.oxfordjournals.org/content/14/2/241.full.pdf <. [Accessed 04.09.2013].

Floyd. Rita (2007) 'Towards a Consequentialist Evolution of Security: Bringing Together the Copenhagen and the Welsh Schools of Security Studies' *Review of International Studies* 2007 33:2, 327-350. >http://journals.cambridge.org/abstract_S026021050700753X<. [Accessed 04.09.2013].

Flynn. Thomas (2005). 'Foucault's Mapping of History' (Ed.) Gutting. Gary (2005) *The Cambridge Companion to Foucault.* Cambridge University Press. Cambridge. United Kingdom.

Foster. Nigel (2006) *Foster on EU Law.* Oxford University Press. Oxford. United Kingdom.

Foster. Nigel (2010) *Blackstone's EU Treaties and Legislation 2010-2011.* Oxford University Press. Oxford. United Kingdom.

Foucault. Michel (1969) *The Archaeology of Knowledge.* Routledge, Abingdon. United Kingdom.

Foucault. Michel (1970) *The Order of Things.* Tavistock. London, United Kingdom

Foucault. Michel (1988) 'The Ethic of Care for the Self as a Practice of Freedom' (Ed.) Bernauer. James and David Rasmussen (1988) *The Final Foucault.* MIT-Press. Boston. United States.

Foucault. Michel (1991) 'Governmentality' (Ed.) Burchell, Graham and Colin Gordon (1991) *The Foucault Effect: Studies in Governmentality*. University of Chicago Press. Chicago. United States.

Foucault. Michel (1994a) 'Governmentality' (Ed.) Faubion. James D. (1994) *Michel Foucault. Power. Essential Works of Foucault 1954 – 1984. Volume 3*. Penguin Books. London. United Kingdom.

Foucault. Michel (1994b) 'Questions of Methods' (Ed.) Faubion. James D. *Michel Foucault. Power. Essential Works of Foucault 1954 – 1984. Volume 3*. Penguin Books. London. United Kingdom.

Foucault. Michel (2009) *Security, Territory, Population. Lectures at the Collège de France 1977 – 1978.* Palgrave Macmillan. Basingstoke. United Kingdom.

Frank. Kasper (2014) 'Hackere lagde flere netværk ned og fik ændret flyrute' [Hackers brought down several networks and changed a flight route] *Jyllands-Poster. Digital. 25.08.2014. Webpage.* >http://jyllands-posten.dk/digitalt/ECE6968045/hackere-lagde-flere-netvaerk-ned-og-fik-aendret-flyrute/<. [Accessed 25.08.2014].

Freestone. David and Ellen Hey (1996) 'Origins and Development of the Precautionary Principle' (Ed.) Freestone. David and Ellen Hey. *The Precautionary Principle and International Law: The Challenge of Implementation.* Kluwer Law International. The Hague. The Netherlands.

Fuerth. Leon (2011) 'Operationalizing Anticipatory Governance' *Prism, 2011 2:4, 31-46.* >http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCEQFjAA&url=http%3A%2F%2Fcco.dodlive.mil%2Ffiles%2F2014%2F02%2FPrism_31-46_Fuerth.pdf&ei=JQzJVInbE8ve7Aa_x4GgBA&usg=AFQjCNEv9dkTTr4rD4YrGV6PgrQUS6uIvw&sig2=uWTmt4OTfiZnFOjwHQg8JQ<. [Accessed 19.12.2014].

Furendi. Frank (2005) *Culture of Fear. Risk-taking and the Morality of Low Expectation*. Continuum. London. United Kingdom.

Galvin. John. R. (1991) 'From Immediate Defence Towards Long-term Stability' *NATO Review no. 6.* >http://www.nato.int/docu/review/1991/9106-3.htm<. [Accessed 03.09.2013].

Garcia Suarez. Marcial A. and Acàcio Igor D. Palhares (2014) 'Reflections on Virtual to Real: Modern Techniques, International Security Studies and Cyber Security Environment' (Ed.) Kremer and Muller (2014) *Cyberspace and International Relations.* Springer-Verlag. Berlin. Germany.

Gardner. Dan (2009) *Risk. The Science and Politics of Fear*. Virgin Books. London. United Kingdom.

Garland. David (1997) ''Governmentality' and the Problem of Crime: Foucault, Criminology, Sociology' *Theoretical Criminology 1997 1:2, 173-214.* >http://tcr.sagepub.com/content/1/2/173.full.pdf<. [Accessed 03.09.2013].

Garland. David (2003) 'The Rise of Risk' (Ed.) Ericson. Richard V. and Aaron Doyle. *Risk and Morality.* University of Toronto Press. Toronto. Canada.

Gearty. Connor (2010) 'Escaping Hobbes: Liberty and Security for Our Democratic (Not Anti-Terrorist) Age' *LSE Law, Society and Economy Working Papers 3/2010.* >http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1543121<. [Accessed 09.01.2015].

Gellman. Barton and Ashkan Soltani (2013) 'NSA Tracking Cellphone Locations Worldwide, Snowden Documents show' *The Washington Post. 04.12.2013.* Webpage. >http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-6ca94801fac_story.html?wpisrc=emailtoafriend. [Accessed 28.04.2014].

Gibbs. Samuel (2014) 'Islamic State Moves to Other Social Networks after Twitter Clampdown' *The Guardian. 21.08.2014. Webpage*. > http://www.theguardian.com/technology/2014/aug/21/islamic-state-isis-social-media-diaspora-twitter-clampdown<. [Accessed 04.08.2014].

Giddens. Anthony (1995) 'Living in a Post-traditional Society' (Ed.) Beck. Ulrich and Anthony Giddens, Scott Lash. *Reflexive Modernization. Politics, Tradition and Aesthetics in the Modern Social Order.* Polity Press. Cambridge. United Kingdom.

Giddens. Anthony (1998) ‘‘Risk Society’: The Context of British Politics’ (Ed.) Franklin. Jane. *The Politics of Risk Society*. Polity Press. Cambridge. United Kingdom.

Gilmour. Gerry J. (2002) ‘Bush: West Point Grads Answer History's Call to Duty’ *The U.S. Department of Defence. D.O.D. News. 01.06.2002. Webpage.* >http://www.defense.gov/news/newsarticle.aspx?id=43798<. [Accessed 05.01.2015].

Giraldo. Jeanne and Harold Trinkunas (2010) ‘Transnational Crime’ (Ed.) Collins. Alan. *Contemporary Security Studies*. Oxford. University Press. Oxford. United Kingdom.

Glaser. Barney and Anselm L. Strauss (2009) *The Discovery of Grounded Theory: Strategies for Qualitative Research.* Transaction Publishers. New Jersey. United States.

Global Organizations (2014) ‘EU Law’ *Webpage.* http://www.cybercrimelaw.net/EU.html<. [Accessed 20.06.2014].

Goldsmith. Andrew (2008) ’The Governance of Terror: Precautionary Logic and Counterterrorist Law Reform after September 11’ *Law & Policy* 2008 30:2, 141-167. >http://onlinelibrary.wiley.com/doi/10.1111/j.1467-9930.2008.00272.x/pdf<. [Accessed 05.09.2013].

Goodman. Seymour E. and Jessica C. Kirk, Megan H. Kirk (2007) ‘Cyberspace as a Medium for Terrorists’ *Technological Forecasting & Social Change* 2007 74:2, 193-210. >http://www.sciencedirect.com/science/article/pii/S004016250600148X<. [Accessed 09.09.2013].

Gordon. Colin (1991) ‘Governmental Rationality: an Introduction’ (Ed.) Graham Burchell, Colin Gordon and Peter Miller (1991) The Foucault Effect: Studies in Governmentality. Hemel Hempstead: Harvester Wheatsheaf. United Kingdom.

Gordon. Sarah and Richard Ford (2002) ‘Cyberterrorism?’ *Computer & Security 2002 21:7, 636-647.* >http://www.sciencedirect.com/science/article/pii/S0167404802011161<. [Accessed 09.09.2013].

Grabosky. Peter (2007a) *Electronic Crime*. Pearson Education Inc. New Jersey. United States.

Grabosky. Peter (2007b) ‘Requirements of Prosecution Services to Deal with Cyber-crime’ *Crime, Law and Social Change 2007, 47:4-5, 201-22, 207.* >http://link.springer.com/article/10.1007%2Fs10611-007-9069-1#page-1<. [Accessed 20.01.2015].

Grabosky. Peter N and Russel G. Smith (2003) ‘Crime in the Digital Age’ (Ed.) Goldsmith. Andrew and Mark Israel and Kathleen Daly (2003) *Crime and justice: an Australian textbook in criminology*. Lawbook Co. Sydney. Australia.

Grabosky. Peter and Michael Stohl (2010) *Crime and Terrorism.* SAGE Publications. London. United Kingdom**.**

Gray. Christine (2004) International Law and the Use of Force. Oxford University Press. Oxford. United Kingdom.

Gray. Collins. S. (2007) *War, Peace and International Relations. An Introduction to Strategic History*. Routledge. Abingdon. United Kingdom.

Grissom. Adam (2006) ‘The future of military innovation studies’ *Journal of Strategic Studies 2006 29:5, 905-934.* >http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved=0CCMQFjAA&url=http%3A%2F%2Fweb.singnet.com.sg%2F~shuhuang%2Fgrissom.pdf&ei=tM3GVP2xBsmxUZbeg7AC&usg=AFQjCNEk3UTgSl_13dQ1Nwug_CvwHyYHpg&sig2=2NP3Wa1DWXCZhqpL4b-FcQ&bvm=bv.84349003,d.d24<.[Accessed 05.01.2015].

Gorman. Michael. E. (2012) ‘A Framework for Anticipatory Governance and Adaptive Management of Synthetic Biology’ *International Journal of Social Ecology and Sustainable Development (IJSESD), 3:2, 64-68.* > http://www.igi-global.com/article/framework-anticipatory-governance-adaptive-management/67360<. [Accessed 10.01.2015].

Government Bill (2014) ‘Counter-Terrorism and Security Bill 2014-15’ *WWW.Parliament.UK.* >http://services.parliament.uk/bills/2014-15/counterterrorismandsecurity.html<. [Accessed 20.01.2015].

Gross. Oren (2000) ’Exception and Emergency Powers: The Normless and Exceptionless Exception: Carl Schmitt’s Theory of Emergency Powers and the “Norm-Exception” Dichotomy’ *Cardozo Law Review 2000 21, 1825-1869.* >http://heinonline.org/HOL/Page?handle=hein.journals/cdozo21&div=78&g_sent=1&collection=journals<. [Accessed 03.09.2013].

Gross. Oren (2009) 'Security vs Liberty: An Imbalanced Balancing' *University of Minnesota Law School Legal Studies Research Paper Series, Research Paper No. 09-42.* >http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471634<. [Accessed 27.08.2014].

Group of 8 (2000) 'G8 Conference on Cybercrime' *Webpage.* >http://www.euractiv.com/en/general/g8-conference-cybercrime/article-114652<. [Accessed 03.09.2013].

Grusin. Richard (2004) 'Premediation' *Criticism 46:1, 17–39.* >http://muse.jhu.edu/journals/criticism/v046/46.1grusin.html<. [Accessed 20.12.2014].

Guba. Egon G. and Yvonna S. Lincoln (1994) 'Competing Paradigms in Qualitative Research' (Ed.) Denzin, Norma K. and Yvonne S. Lincoln (1994) *Handbook of Qualitative Research*, Sage Publications. Newbury Park. Canada.

Gunderson. Lance. H. and C.S. Holling, Lowell Pritchard Jr, Garry D. Peterson (2002) 'Resilience of Large-Scale Resource Systems' (Ed.) Gunderson Lowell H. and L. Pritchard Jr. *Resilience and the Behaviour of Large-Scale Systems*. Island Press. Washington, DC. United States.

Guston. David. H. (2014) 'Understanding 'Anticipatory Governance' *Social Studies of Science 2014 44:2, 218-142.* >http://sss.sagepub.com/content/44/2/218.full.pdf+html<. [Accessed 26.12.2014].

Gutting. Gary (1994) 'Michel Foucault. A User's Manual'(Ed.) Gutting. Gary (2014) *The Cambridge Companion to Foucault.* Cambridge University Press. Cambridge. United Kingdom.

Hacking. Ian (2003) 'Risk and Dirt' (Ed.) Ericson. Richard V. and Aaron Doyle. *Risk and Morality.* University of Toronto Press. Toronto. Canada.

Haftendorn, Helga and Robert Keohane, Celeste Wallander (1999) *Imperfect Unions: Security Institutions Over Time and Space: Security Institutions Over Time and Space.* Oxford University Press. Oxford. United Kingdom.

Haimes. Yacov Y. (2006) 'On the Definition of Vulnerabilities in Measuring Risks to Infrastructures' *Risk Analysis 2006 26:2, 293-396.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2006.00755.x/pdf<. [Accessed 06.09.2013].

Halliday. Josh and Charles Arthur (2010) 'WikiLeaks: Anonymous Hierarchy Emerges' *The Guardian. Webpage.* 16.12.2010. http://www.theguardian.com/media/2010/dec/16/wikileaks-anonymous-hierarchy-emerges<. [Accessed 20.04.2014].

Hansen. Lene (2013) *Security as Practice: Discourse Analysis and the Bosnian War.* Routledge. Abington. United Kingdom.

Hansen. Lene and Helen Nissenbaum (2009) 'Digital Disaster, Cyber Security and the Copenhagen School' *International Studies Quarterly 53, 1555-1575.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2478.2009.00572.x/pdf<.

Hart. Caterine (2011) 'Mobilizing the Cyber Space Race: the Securitization of the Internet and its Implications for Civil Liberties' *The Securitization in Everyday Life: An International Workshop.* >http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.digitallymediatedsurveillance.ca%2Fwp-content%2Fuploads%2F2011%2F04%2FHart-Mobilizing-the-Cyberspace-race.pdf&ei=Q1XJVN7cDYOt7Aa2rYGwCQ&usg=AFQjCNGQi2zIHquSkPPTVrmZ_i53RwwJSA&sig2=oURFi7gLl-W0rnhYL0FtOg&bvm=bv.84607526,d.ZGU<. [Accessed 12.01.2015].

Hart. Christopher (1998) *Doing a Literature Review: Releasing the Social Science Research Imagination*. Sage. London. United Kingdom.

Hartung. William D. (1998) 'Reagan Redux: The Enduring Myth of Star Wars' *World Policy Journal 1998 15:3,17-24.* >http://www.jstor.org/stable/40204776<. [Accessed 24.08.2014].

Haubrich. Dirk (2006) 'Anti-terrorism Laws and Slippery Slopes: A Reply to Waddington' *Policing and Society 2006 16:4, 405-421* >http://www.tandfonline.com/doi/full/10.1080/10439460600973719#.VCVuPvldVqU<. [Accessed 17.12.2014].

Haugaard. Mark (2002) 'Foucault' (Ed.) Haugaard. Mark (2002) *Power. A Reader*. Manchester University Press. Manchester. United Kingdom.

Hawkins. Steve and David C. Yen, David C. Chou (2000) 'Awareness and Challenges of Internet Security' *Information Management and Computer Security 2000 8:3, 131-143.* >http://www.emeraldinsight.com/journals.htm?articleid=862768<. [Accessed 12.09.2013].

He. Qizhi (1995) 'The Crucial Role of the United Nations in Maintaining International Peace and Security' (Ed.) Christian Tomuscha. *The United Nations at Age Fifty: A Legal Perspective*. Kluwer Law International. The Hague. The Netherlands.

Healy. Marilyn and Chad Perry (2000) 'Comprehensive Criteria to Judge Validity and Reliability of Qualitative Research within the Realism Paradigm' *Qualitative Market Research: An International Journal 2000 3,118 – 126.* >http://dx.doi.org/10.1108/13522750010333861<. [Accessed 20.12.2014].

Hebenton. Bill and Toby Seddon (2009) 'From Dangerousness to Precaution. Managing Sexual and Violent Offenders in an Insecure and Uncertain Age' *British Journal of Criminology. 2009 49, 343-362.* >http://bjc.oxfordjournals.org/content/49/3/343.full.pdf<. [Accessed 04.09.2013].

Heng. Yee-Kuang (2006) 'The 'Transformation of War' Debate: Through the Looking Glass of Ulrich Beck's World Risk Society' *International Relations 2006 20: 69.* >http://ire.sagepub.com/content/20/1/69.full.pdf<. [Accessed 09.09.2013].

Hern. Alex (2013) 'A History of Bitcoin Hacks' *The Guardian, 18.03.2014. Webpage.* >http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency<. [Accessed 10.08.2014].

Hern. Alex (2014) 'Heartbleed: Hundreds of Thousands of Servers at Risk from Catastrophic Bug' *The Guardian, 09.04.2014. Webpage.* >http://www.theguardian.com/technology/2014/apr/08/heartbleed-bug-puts-encryption-at-risk-for-hundreds-of-thousands-of-servers<. [Accessed 12.08.2014].

Hildebrandt. Mirelle (2008) 'A Vision of Ambient Law' (Ed.) Brownsword, Roger and Karen Yeung. *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*. Hart Publishing. Oxford. United Kingdom.

Hiller. Janine S. and Roberta S. Russell (2013) 'The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison' *Computer Law & Security Review 2013 29:3, 236-245.* >http://www.sciencedirect.com/science/article/pii/S0267364913000575<. [Accessed 05.10.2014].

Hindess. Barry (1996) *Discourses of Power. From Hobbes to Foucault*. Blackwell. Oxford. United Kingdom.

Hirst. Paul (2001) *War and Power in the 21st Century*. Polity Press. Cambridge. United Kingdom.

Hopkins. Nick (2013) 'UK Gathering Secret Intelligence via Covert NSA Operation' *The Guardian. 07.06.2013. Webpage.* >http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism<. [Accessed 25.04.2014].

Hopkins. Nick and Luke Harding (2013) 'Pro-Assard Syrian Hackers Launching Cyber-attacks on Western Media'. *The Guardian. 29.04.2013. Webpage.* >http://www.theguardian.com/world/2013/apr/29/assad-syrian-hackers-cyber-attacks/print<. [Accessed 09.09.2013].

Holling. C.S. (1973) 'Resilience and the Stability of Ecological Systems' *Annual Review of Ecology and Systematics 1973 4:1, 23.* >http://www.annualreviews.org/doi/abs/10.1146/annurev.es.04.110173.000245<. [Accessed 09.01.2015].

Hough. Peter (2008) *Understanding Global Security*, Routledge. Abingdon. United Kingdom.

Humphreys. Adam R.C. (2010) 'The Heuristic Application of Explanatory Theories in International Relations' *European Journal of International Relations 2011 17: 2, 257–277.* >http://ejt.sagepub.com/content/17/2/257.full.pdf<. [Accessed 09.09.2013].

Huysmans. Jef (1998) 'Security! What do You Mean?: From Concept to Thick Signifier' *European Journal of International Relations 1998; 4:2, 226-255.* >http://ejt.sagepub.com/content/4/2/226.full.pdf+html <. [Accessed 03.09.2013].

Huysmans. Jef (2006) 'Agency and the Politics of Protection. Implications for Security Studies' (Ed.) Huysmans. Jef, and Andrew Dobson, Raia Prokhovnik. *Politics of Protection. Sites of Insecurity and Political Agency.* Routledge. Abingdon. United Kingdom.

Huysmans. Jef (2006) *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. Routledge. London. United Kingdom

Independent Commission on International Development Issues (1980) *North-South: A Programme for Survival. The Report of the International Commission on International Development Issues*. Pan Books. London. United Kingdom.

Interpol (2013) ‘Cybercrime’ *Crime Areas. Webpage.* >http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime<. [Accessed 09.09.2013].

ITU (2014) ‘Cyber Security Definition’ *Webpage.* >http://www.itu.int/en/ITU-/studygroups/com17/Pages/cybersecurity.aspx<. [Accessed 02.02.2014].

Jackson. Richard (2005) *Writing the War on Terrorism. Language, Politics and Counter-terrorism.* Manchester University Press. Manchester. United Kingdom.

Johnson. Les (1992) *The Rebirth of Private Policing*. Routledge. London. United Kingdom.

Johnson. Les (2006) ‘Transnational Security Governance**’** (Ed.) Wood. Jennifer and Benoît Dupont. *Democracy, Society and the Governance of Security*. Cambridge University Press. Cambridge. United Kingdom.

Jones. Andrew (2005) ‘Cyber Terrorism: Fact or Fiction’ *Computer Fraud & Security 2005 6, 4-7.* >http://www.sciencedirect.com/science/article/pii/S1361372305702207#<. [Accessed 09.09.2013].

Jordan. Tim (2013) *Hacking: Digital Media and Technological Determinism*. John Wiley & Sons. London. United Kingdom.

Jordan. Tim and Paul A. Taylor (2004) *Hacktivism and Cyberwars. Rebels with a Cause*? Routledge. London. United Kingdom.

Jordana. Jacint and David Levi-Faur (2004) *Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance.* Edward Elgar, Cheltenham. United Kingdom.

Joseph. Jonathan (2013) ‘Resilience in the UK and French Security Strategy: An Anglo-Saxon Bias?’ *Research Article. Political Studies Association 2013 1-12.* >http://onlinelibrary.wiley.com/doi/10.1111/1467-9256.12010/pdf<. [Accessed 06.09.2013].

Kaldor. Mary (2013) *Human security*. John Wiley & Sons. London. United Kingdom.

Karinen. Risto and David H. Guston (2010) ‘Toward Anticipatory Governance: The Experience with Nanotechnology’ (Ed.) Kaiser, Mario and Monka Kurath, Sabine Maasen, Christoph Rehmann-Sutter (2010) *Governing Future Technologies. Nanotechnology and the Rise of an Assessment Regime.* Springer. Netherlands. >http://link.springer.com/chapter/10.1007/978-90-481-2834-1_12<. [Accessed 10.01.2015].

Kassab. Hanna Samir (2014) ‘In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare’ (Ed.) Kremer. Jan-Frederik and Benedikt Müller (2014) *Cyber Space and International Relations: Theory, Prospects and Challenges*. Springer-Verlag. Berlin. Germany.

Kaunert. Christian (2011) ‘European Internal Security-towards Supranational Governance in the Area of Freedom, Security and Justice?’. Manchester University Press, Manchester. United Kingdom.

Kelion. Leo (2014a) ‘eBay makes Users Change their Passwords after Hack’ *Technology,* 21.05.2014. *Webpage.* >http://www.bbc.co.uk/news/technology-27503290<. [Accessed 11.08.2014].

Kelion. Leo (2014b) ‘Feedly and Evernote Struck by Denial of Service Cyber-attacks’ *News. 11.06.2014. Webpage.* >http://www.bbc.co.uk/news/technology-27790068<. [Accessed 27.07.2014].

Kendall. Gavin (2004) ’Global, International and Actor Network’ (Ed.) Larner. Wendy and William Walters. *Global Governmentality. Governing International Spaces*. Routledge. Abingdon. United Kingdom.

Kerr. Pauline (2010) ’Human Security’ (Ed.) Collins. Alan. *Contemporary Security Studies*. Oxford University Press. Oxford. United Kingdom.

Keyser. Mike (2002) ‘The Council of Europe Convention on Cybercrime’ *Journal of Transnational Law and Policy 2002 12, 287.* >http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jtrnlwp12&section=14<. [Accessed 15.12.2014].

King. Gary and Christopher J. Murray (2001) ‘Rethinking Human Security’*Political Science Quarterly 2001 116:4, 585-610.* >http://onlinelibrary.wiley.com/doi/10.2307/798222/pdf<. [Accessed 20.07.2014].

King. Nancy J. and V.T. Raja (2012) 'Protecting the Privacy and Security of Sensitive Customer Data in the Cloud'. *Computer Law & Security Review 2012 28:3, 308-319.* >http://www.sciencedirect.com/science/article/pii/S0267364912000556<. [Accessed 15.12.2014].

Kjær Anne Mette (2004) *Governance*. Polity Press. Cambridge. United Kingdom.

Klimburg. Alexander (2009) 'Cyber-attacken als Warnung. Wer hat die Website des US-Präsidenten lahmgelegt?' [Cyber-attacks as a Warning, where has the Webpage Paralyzed the US President?]. *DiePress. Print-Ausgabe. 10.07.2009.* >http://diepresse.com/home/meinung/gastkommentar/493918/CyberAttacken-als-Warnung<. [Accessed 20.04.2014].

Klimburg. Alexander (2011) 'Mobilising Cyber Power' *Survival: Global Politics and Strategy 2011 53:1, 41-60.* >http://www.tandfonline.com/doi/pdf/10.1080/00396338.2011.555595<. [Accessed 09.09.2013].

Knapp. Kenneth J. and William R. Boulton (2006) 'Cyber-warfare Threatens Corporations: Expansion into Commercial Environments' *Information System Management 2006 23:3, 76-87.* >http://www.tandfonline.com/doi/pdf/10.1201/1078.10580530/45925.23.2.20060301/92675.8<. [Accessed 06.09.2013].

Knell. Yolande (2012) 'New Cyber Attacks Hits Israeli Stock Exchange and Airline'. *World. 16.01.2012. Webpage.* >http://www.bbc.co.uk/news/world-16577184<. [Accessed 09.09.2013].

Kock. Christian and Martine Buser (2006) 'Emerging Metagovernance as an Institutional Framework for Public Private Partnership Networks in Denmark' *International Journal of Project Management 2006 24:7, 548-556.* >http://www.sciencedirect.com/science/article/pii/S0263786306000895<. [Accessed 08.09.2013].

Konstadinides. Theodore and Noreen O'Meara (2014) 'Fundamental Rights and Judicial Protection (Ed.) Arcarazo. Diego Acosta and Cian Murphy (2014) *EU Security and Justice Law. After Lisbon and Stockholm*. Hart Publishing. Oxford. United Kingdom.

Koops. Bert-Jaap (2008) 'Criteria for Normative Technology. The Acceptability of 'Code as Law' in Lights of Democratic and Constitutional Values' (Ed.) Brownsword. Roger and Karen Yeung (2008) *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes.* Hart Publishing. Oxford. United Kingdom.

Kremer. Jens (2014) 'Policing Cybercrime or Militarizing Cybersecurity? Security Mindsets and the Regulation of Threats from Cyberspace' *Information & Communications Technology Law 2014 23:3, 2020-237.* >http://www.tandfonline.com/eprint/Un9IYdmH9PYNtwS2zW2F/full#.VItGffmzmM9<. [Accessed 14.12.2014].

Lakoff. Andrew (2006) 'Techniques of Preparedness' (Ed.) Monahan. Torin (2006) *Surveillance and Security; Technological Politics and Power in Everyday Life.* Routledge. New York. United States.

Lakoff. Andrew and Stephen J. Collier (2010) 'Infrastructure and event: the political technology of preparedness'. *Political Matter: Technoscience, Democracy, and Public Life* 2010, 243-266.

Lauren, Paul Gordon (2011) *The Evolution of International Human Rights: Visions Seen*. University of Pennsylvania Press. Pennsylvania. United States.

Laville. Sandra (2012) 'Anonymous Cyber-attacks Cost PayPal £3.5m, Court Told' *The Guardian* 22.11.2012. . >http://www.guardian.co.uk/technology/2012/nov/22/anonymous-cyber-attacks-paypal-court<. [Accessed 12.09.2013].

Lawson. Sean (2012) 'Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States' *First Monday 2012 17,7.* >http://firstmonday.org/ojs/index.php/fm/article/viewArticle/3848<. [Accessed 20.12.2014].

Leander. Anna (2005) 'The Power to Construct International Security: On the Significance of Private Military Companies' *Millennium – Journal of International Studies 2005 33:3, 803-825.* >http://mil.sagepub.com/content/33/3/803.full.pdf+html<. [Accessed 06.09.2013].

Lemke. Thomas (2000) 'Foucault, Governmentality, and Critique'. *Paper presented at the Rethinking Marxism Conference, University of Amherst (MA), September 21-24, 2000.* >http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved=0CCMQFjAA&url=http%3A%2F%2Fwww.thomaslemkeweb.de%2Fpublikationen%2FFoucault%2C%2520Governmentality%2C%2520and%2520Critique%2520IV-2.pdf&ei=-cbGVOCgBoXnUujmgbgH&usg=AFQjCNEGducF-

lLUEXKYWxARUkDNma9JQg&sig2=AQASBjc6iMOSLccECjy9bg&bvm=bv.84349003,d.d24<. [Accessed 20.01.2015].

Lemke. Thomas (2001) 'The Birth of Bio-politics: Michael Foucault's Lectures at the College de France on Neo-liberal Governmentality' *Economy and Society 30:1.* >http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved=0CCMQFjAA&url=http%3A%2F%2Fwww.thomaslemkeweb.de%2Fengl.%2520texte%2FThe%2520Birth%2520of%2520Biopolitics%25203.pdf&ei=A_PHVJe7Juiy7QbVsoGoBQ&usg=AFQjCNGWAa70w83ouJ4MEreNp36MlOeSAg&sig2=EUkxwiK56vDweEIX5wJCbA&bvm=bv.84349003,d.ZGU<.[Accessed 20.01.2015].

Lenaerts. Koen. (2012) 'Exploring the Limits of the EU Charter of Fundamental Rights' *European Constitutional Law Review, 2012 8:03, 375-403.* >http://journals.cambridge.org/abstract_S1574019612000260<. [Accessed 20.01.2015].

Lentzos. Filippa and Nikolas Rose (2009) 'Governing Insecurity: Contingency Planning, Protection, Resilience' *Economy and Society* 2009 38:2, 230-254. >http://www.tandfonline.com/doi/pdf/10.1080/03085140902786611<. [Accessed 03.09.2013].

Lessing. Lawrence (1998) *Code and Other Laws of Cyberspace*. Basic Books. Harvard. United States.

Lessing. Lawrence (1999) 'The law of the horse: What cyberlaw might teach' Harvard law review 1999 113:2 501-549. >http://www.jstor.org/stable/1342331?seq=1#page_scan_tab_contents<. [Accessed 01.02.2014].

Levi. Michael and David S. Wall (2004) 'Technologies, Security, and Privacy in the Post-9/11 European Information Society' *Journal of Law and Society 2004 31:2,194-220.*>http://onlinelibrary.wiley.com/doi/10.1111/j.1467-6478.2004.00287.x/full<.

Levy. Marc A. (1995) 'Is the Environment a National Security Issue?' *International Security 1995 20:2, 35-62.* >http://www.jstor.org/stable/pdfplus/2539228.pdf<. [Accessed 03.09.2013].

Lewis. Paul and Spencer Ackerman, Ian Cobain (2014) 'Steven Sotloff: Isis Video Claims to show Beheading of US Journalist' *The Guardian. 03.09.2014. Webpage.* >http://www.theguardian.com/world/2014/sep/02/isis-video-steven-sotloff-beheading<. [Accessed 04.09.2014].

Linder. Stephen H. (1999) 'Coming to Terms with the Public-Private Partnership: A Grammar of Multiple Meanings' *American Behavioural Scientist 1999 43:1 35-51.* >http://abs.sagepub.com/content/43/1/35.full.pdf+html<. [Accessed 04.09.2013].

Lippmann. Walter (1943) *US Foreign Policy*. Hamish Hamilton. London. United Kingdom.

Litwak. Robert S. (2003) 'The New Calculus of Pre-emption' *Survival 2003 44:4, 53-80.* >http://www.tandfonline.com/doi/pdf/10.1080/00396330212331343492<. [Accessed 12.09.2013].

Loader. Ian (1999) 'Consumer Culture and the Commodification of Policing and Security' *Sociology 1999 33:2, 373-392.* >http://soc.sagepub.com/content/33/2/373.full.pdf+html<.

Loader. Ian and Neil Walker (2006) 'Necessary Virtues: the Legitimate Place of the State in the Production of Security' **(**Ed.) Wood. Jennifer and Benoît Dupont. *Democracy, Society and the Governance of Security.* Cambridge University Press. Cambridge. United Kingdom.

Loader. Ian and Neil Walker (2007) *Civilizing Security*. Cambridge University Press. Cambridge. United Kingdom.

Lodge. Martin (2004) 'Accountability and Transparency in Regulation: Critiques, Doctrines and Instruments', (Ed.). Jacint Jordana and David Levi-Faur (2004) *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance.* Edward Elgar, Cheltenham. United Kingdom.

Long. Edward and Franklin, Aimee L. (2004) 'The Paradox of Implementing the Government Performance and Results Act: Top-Down Direction for Bottom-Up Implementation' *Public Administration Review, 2004 64: 3, 309–319.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1540-6210.2004.00375.x/pdf<. [Accessed 12.12.2014].

Lopes. Lola. L. (1987) 'Between Hope and Fear: the Psychology of Risk' (Ed) Leonard Berkowitz (1987) *Advance in Experimental and Social Psychology*. Academic Press. San Diego. United States.

Luhmann. Niklas (1993) *Risk: A Sociological Theory*. Walter de Gruyter. New York. United States.

Lukasik. Stephen. J. and Seymour E. Goodman, David W. Longhurst (2003) 'Protecting Critical Infrastructure against Cyber-Attack' Oxford University Press. Oxford. United Kingdom.

Lund Petersen. Karen (2011) ‘Risk Analysis – A Field within Security Studies?’ *European Journal of International Relations* 2011 18:4, 693-717. >http://ejt.sagepub.com/content/18/4/693.full.pdf+html<. [Accessed 12.09.2013].

Lundborg. Tom and Nick Vaughan-Williams (2011) ‘Resilience, Critical Infrastructure, and Molecular Security: The Excess of “Life” in Biopolitics *International Political Sociology* 2011 5:367–383. >http://onlinelibrary.wiley.com/doi/10.1111/j.1749-5687.2011.00140.x/full<. [Accessed 27.05.2015].

Lupton. Deborah (1999) *Risk*. Routledge. Abingdon. United Kingdom.

Lupton. Deborah (2006) ’Sociology and Risk’ (Ed.) Mythen. Gabe and Sandra Walklate. *Beyond the Risk Society. Critical Reflections on Risk and Human Security.* Open University Press. Maidenhead. United Kingdom.

Lyall. Catharine and Joyce Tait (2005b) ‘Shifting Policy Debates and the Implications for Governance’ (Ed.) Lyall. Catharine and Joyce Tait (2005) *New Modes of Governance. Developing an Integrated Policy Approach to Science, Technology, Risk and the Environment.* Ashgate. London. United Kingdom.

MacAskill. Ewen (2010) ‘US 'Star Wars' Lasers bring down Ballistic Missile’ *The Guardian. 12.02.2010. Webpage.* >http://www.theguardian.com/science/2010/feb/12/star-wars-laser-ballistic-missile<. [Accessed 24.08.2014].

MacAskill, Ewen and Julian Borger, Nick Hopkins, Nick Davies, James Ball (2013a) ‘GCHQ taps Fibre-optic Cables for Secret Access to World's Communications’ *The Guardian. 21.06.2013. Webpage.* >http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa<. [Accessed 25.04.2014].

MacAskill, Ewen and Julian Borger, Nick Hopkins, Nick Davies and James Ball (2013b) ‘Mastering the Internet: how GCHQ set out to Spy on the World Wide Web’ *The Guardian. 21.06.2013. Webpage*. http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet<. [Accessed 07.12.2014].

McCulloch. Jude and Sharon Pickering (2009) ‘Pre-Crime and Counter-Terrorism: Imagining Future Crime in the “War on Terror”’ *British Journal of Criminology* 2009 49, 628–645 >http://bjc.oxfordjournals.org/content/49/5/628.full.pdf<. [Accessed 07.09.2013].

McCurry. Justin (2014a) ‘South Korean nuclear operator hacked amid cyber-attack fears’. The Guardian. 23.12.2014. Webpage. >http://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack<. [Accessed 23.12.2014].

McCurry. Justin (2015b) ‘Isis Video Purports to Show Beheading of Japanese Hostage Kenji Goto’ *The Guardian. 31.01.2015. Webpage*. >http://www.theguardian.com/world/2015/jan/31/isis-video-beheading-japanese-hostage-kenji-goto<. [Accessed -3.02.2015].

McCusker. Rob (2006) ‘Transnational Organized Cyber Crime: Distinguishing Threat from Reality’ *Crime Law and Social Change 2006 46:4-5, 257-273.* >http://link.springer.com/content/pdf/10.1007%2Fs10611-007-9059-3.pdf<. [Accessed 08.09.2013].

McDonald. Matt (2008b) ‘Securitization and the Construction of Security’ *European Journal of International Relations* 2008 14:4, 563-587. >http://ejt.sagepub.com/content/14/4/563.full.pdf+html< [Accessed 03.09.2013].

McIntyre M. J. and Colin Scott (2008) ‘Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility’ (Ed.) Brownswood. Roger and Karen Yeung (2008) *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*. Hart Publishing. Oxford. United Kingdom.

McMillan. Robert (2008) ‘Hackers Hit Scientology With Online Attack’ *PCWorld News*. *26.01.2008. Webpage.* >http://www.pcworld.com/article/141839/article.html<. [Accessed 09.09.2013].

Mansfield-Devine. Steve (2011) ‘Hacktivism: Assessing the Damage’ *Network Security 2011 2011:8, 5-13.* >http://www.sciencedirect.com/science/article/pii/S1353485811700848<. [Accessed 08.09.2013].

Maras. Marie-Helen (2014) ‘Inside Darknet: the Takedown of Silk Road: Marie-Helen Maras Reports on the Unexplored Underworld of Cyberspace’ *Criminal Justice Matters 2014 98: 1, 22-23.* >http://www.tandfonline.com/doi/abs/10.1080/09627251.2014.984541#.VMorPfmzmM8<. [Accessed 12.01.2015].

Margretts. Helen Z. (2009) ‘The Internet and Public Policy’ *Policy & Internet 2008 1:4, 1-21.* >http://www.psocommons.org/policyandinternet/vol1/iss1/art1/<. [Accessed 10.09.2013].

Marion. Nancy E. (2010) ‘The Council of Europe’s Cyber Crime Treaty: An Exercise in Symbolic Legislation’ *International Journal of Cyber Criminology 2010 4:1-2, 699-712.* >http://www.cybercrimejournal.com/marion2010ijcc.pdf<. [Accessed 09.09.2013].

Marinos. L. and A. Sfakianakis (2012) ‘ENISA Threat Landscape Responding to the Evolving Threat Environment [Deliverable – 2012-09-28]’ *ENISA Report.* >http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape<. [Accessed 09.09.2013].

Marshaw. Jerry (2006) ‘Accountability and Institutional Design: Some Thoughts on the Grammar of Governance‘ (Ed.) Dowdle. Michael W. (2006) *Public Accountability, Designs, Dilemmas and Experiences*. Cambridge University Press. Cambridge. United Kingdom.

Masters. Greg (2010) ‘Global Cybercrime Treaty Rejected at U.N.’ *SG Magazine for IT Professionals. 23. April 2010.* >http://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/#<. [Accessed 10.09.2013].

Matland. Richard E. (1995) ‘Synthesizing the Implementation Literature: The Ambiguity-Conflict Model of Policy Implementation’ *Journal of Public Administration, Research and Theory 1995 5:2, 145-174.* >http://jpart.oxfordjournals.org/content/5/2/145.full.pdf+html<. [Accessed 08.12.2014].

May. Peter (2007) ‘Regulatory Regimes and Accountability’ *Regulation and Governance 2007 1, 8-26.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1748-5991.2007.00002.x/pdf<. [Accessed 12.09.2014].

Mazmanian. Daniel and Sabatier. Paul A. (1983) *Implementation and Public Policy*. Scott, Foresman Glenview. United States.

Mazmanian. Daniel and Sabatier. Paul A (1989) *Implementation and Public Policy, Reviewed Edition*. University Press of America. Larham. United States.

Microsoft (2014) ‘Microsoft Enters into New Global Partnerships in Fight against Cybercrime’ *Press release. Webpage.* >http://www.microsoft.com/en-us/news/press/2014/feb14/02-12cybercrimepr.aspx<. [Accessed 10.07.2014].

Miller. Peter and Nikolas Rose (2008) *Governing the Present*. Polity Press. Cambridge. United Kingdom.

Miller. Joe (2014a) ‘Apple iCloud Security Exploit is a Concern, Experts Say’ *BBC News. Technology. 03.09.2014. Webpage.* >http://www.bbc.co.uk/news/technology-29045789<. [Accessed 04.09.2014].

Miller. Joe (2014b) ‘Can Iraqi militants be kept off social media sites?’ *BBC News. Technology. 25.06.2014. Webpage.* >http://www.bbc.co.uk/news/technology-28016834<. [Accessed 20.12.2014].

Mills. Albert J, and Gabrielle Durepos, Elden Wiebe (2010) *Encyclopaedia of Case Study Research*. Sage Publications. California.

Mitnick. Kevin and William L. Simon (2013) *Ghost in the Wires: My adventures as the World’s Most Wanted Hacker.* Little, Brown and Company. New York. United States.

Moffatt. Mike (2014) ‘Ponzi Scheme’ *About Education. Economic Categories. Webpage.* >http://economics.about.com/od/financialmarkets/f/ponzi_scheme.htm<. [Accessed 20.12.2014].

Moran. Michael (2002) ‘Understanding the Regulatory State’ *British Journal of Political Science 2002 32:2, 391-413.* >http://www.jstor.org/stable/pdfplus/4092224.pdf?acceptTC=true<. [Accessed 09.09.2013].

Morris. Julian (2000) ‘Defining the Precautionary Principle’ (Ed.) Morris. Julian (2000) *Rethinking Risk and the Precautionary Principle*, Butterworth-Heinemann. Oxford. United Kingdom.

Moore, Tyler, Richard Clayton, and Ross Anderson (2009) ‘The Economics of Online Crime’ *The Journal of Economic Perspectives 2009 23:3,3-20.* >http://www.ingentaconnect.com/content/aea/jep/2009/00000023/00000003/art00001<. [Accessed 20.12.2014].

Mount. Mike (2012) ‘New Cyber Attacks on U.S. Banks; Iran Suspected’ *CNN. Cyber Clearance***.** 18.10.2012. *Webpage.* >http://security.blogs.cnn.com/2012/10/18/new-cyber-attacks-on-u-s-banks-iran-suspected/<. [Accessed 12.09.2013].

Mulgan. Richard (2000) ‘Accountability: An Ever-Expanding Concept?’ *Public Administration 78, 555-573.* >http://onlinelibrary.wiley.com/doi/10.1111/1467-9299.00218/pdf<. [Accessed 04.02.2015].

Mulgan. Richard (2003) *Holding Power to Account: Accountability in Modern Democracies*. Palgrave, London. United Kingdom.

Murkans. Jo Eric Khushal (2009) 'The Quest for Constitutionalism in the UK Public Law Discourses' *Oxford Journal of Legal Studies 2009 29, 427-455.* >http://www.lexisnexis.com/uk/legal/auth/bridge.do?rand=0.23971517308098755<. [Accessed 19.01.2015].

Murray. Andrew and Scott. Colin (2002) 'Controlling the New Media: Hybrid Responses to New Forms of Power' *The Modern Law Review 2002 65:4, 491–516.* >http://onlinelibrary.wiley.com/doi/10.1111/1468-2230.00392/abstract<. [Accessed 06.08.2014].

Mythen. Gabe (2004) *Ulrich Beck. A Critical Introduction to the Risk Society*. Pluto Press. London. United Kingdom.

Mythen, Gabe (2015) 'The Problem of Governance in the Risk Society: Envisaging Strategies, Managing Not-knowing' (Ed.) Urbano Fra. Paleo (2015) *Risk Governance. The Articulation of Hazard, Politics and Ecology.* Springer, The Netherlands.

Mythen Gabe and Sandra Walklate (2006) *Beyond the Risk Society: Critical Reflections on Risk and Human Security*. McGraw Hill, London. United Kingdom.

Mythen. Gabe and Sandra Walklate (2006) 'Criminology and Terrorism. Which Thesis? Risk Society or Governmentality?' *British Journal of Criminology* 2006: 46:3, 379-398. >http://bjc.oxfordjournals.org/content/46/3/379.full.pdf+html<. [Accessed 04.09.2013].

Mythen. Gabe and Sandra Walklate (2008) 'Terrorism, Risk and International Security: The Perils of Asking 'What If?' *Security Dialogue 2008 39: 2-3, 221-242.* >http://sdi.sagepub.com/content/39/2-3/221.full.pdf+html<. [Accessed 04.09.2013].

Mythen. Gabriel and Palash Kamruzzaman (2010) 'Counter-terrorism and Community Relations' (Ed.) Quirk. Hannah and Toby Seddon, Graham Smith (2010) *Regulation and Criminal Justice. Innovations in Policy and Research.* Cambridge University Press, Cambridge. United Kingdom.

Nakashima. Ellen (2013) 'U.S. and Russia Sign Pact to Create Communication Link on Cyber Security' *The Washington Post. National Security. 17.06.2013. Webpage.* >http://articles.washingtonpost.com/2013-06-17/world/40025979_1_cyber-security-pact-homeland-security<. [Accessed 15.09.2013].

Neal. Andrew. W. (2008) 'Goodbye War on Terror? Foucault and Butler on Discourses of Law, War and Exceptionalism' (Ed.) Dillon. Michael and Andrew W. Neal (2008) *Foucault on Politics, Security and War*. Palgrave MacMillian. Basingstroke. United Kingdom.

Neal. Andrew W. (2010) *Exceptionalism and the Politics of Counter-terrorism. Liberty, Security and the War on Terror.* Routledge. Abingdon. United Kingdom.

Neal. Andrew W. (2012a) **'**Normalization and Legislative Exceptionalism: Counterterrorist Lawmaking and the Changing Times of Security Emergencies' *International Political Sociology 2012 6, 260–276.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1749-5687.2012.00163.x/pdf<. [Accessed 04.09.2013].

Neal. Andrew W. (2012b) 'Terrorism, Lawmaking, and Democratic Politics: Legislators as Security Actors' *Terrorism and Political Violence 2012 24:3, 357–374.* >http://www.tandfonline.com/doi/pdf/10.1080/09546553.2011.628721<. [Accessed 20.12.2014].

New America Foundation (2012) 'Future Tense Event: Defining Resilience'. >http://www.newamerica.net/events/2012/defining_resilience<. [Accessed 12.12.2014].

Newman. Edward (2004) 'A Normatively Attractive but Analytically Weak Concept' *Security Dialogue* 2004 35:3, 358-359. >http://sdi.sagepub.com/content/35/3/358.full.pdf<. [Accessed 03.09.2013].

Newman. Janet (2001) *Modernising Governance. New Labour, Policy and Society,* Sage. London. United Kingdom

News in English. No (2014) 'Extent of Cyber Attacks Revealed' *News. 09.07.2014. Webpage.* >http://www.newsinenglish.no/2014/07/09/extent-of-cyber-attacks-revealed/<. [Accessed 27.07.2014].

NewsMax (2014) 'Hackers Took Down Sony's PlayStation Network To Show Lax Security' *25.11.2014. Webpage.* >http://www.Newsmax.com/US/hackers-sony-security-breach/2014/08/25/id/590719/#ixzz3QrdeLTII< **.** [Accessed 12.12.2014].

9/11 Commission (2004) ‘Final Report of the National Commission on Terrorist Attacks upon the United States’. Washington, DC. *National Commission on Terrorist Attacks 26(1): 23–37.* >http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CCgQFjAB&url=http%3A%2F%2Fwww.gpo.gov%2Ffdsys%2Fpkg%2FGPO-911REPORT%2Fpdf%2FGPO-911REPORT.pdf&ei=YRbJVOu_Gu-O7AacloCAAw&usg=AFQjCNEAMI7zbtooXHHMNyUjYQZndhDPDQ&sig2=9D2I-2hlHRKGWr5XbzgUUw&bvm=bv.84607526,d.ZGU<. [Accessed 12.01.2015].

Nissenbaum. Helen (2005) ‘Where Computer Security meets National Security’ *Ethics and Information Technology 2005 7:2, 61-73.* > http://link.springer.com/article/10.1007/s10676-005-4582-3#page-1< .[Accessed 12.12.2014].

Norris. Fran H. and Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, Rose L. Pfefferbaumet (2008) ‘Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness’ *American journal of community psychology* 2008 41:1-2, 127-150. >http://link.springer.com/article/10.1007/s10464-007-9156-6<. [Accessed 27.05.2015].

North Atlantic Treaty Organization (2011b) ‘New Threats: the Cyber Dimension’ *NATO Review Magazine. Webpage.* >http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm<. [Accessed 12.09.2013].

North Atlantic Treaty Organization (2013) ‘Partnership: A Cooperative Approach to Security’ *Webpage.* >http://www.nato.int/cps/en/SID-CAC1FF2F-8AFAA2B4/natolive/topics_84336.htm?<. [Accessed 09.09.2013].

North Atlantic Treaty Organization (2014a) ‘NATO and Cyber Defence’ *Home. Webpage.* >http://www.nato.int/cps/en/natolive/topics_78170.htm<. [Accessed 25.04.2014].

North Atlantic Treaty Organization (2014b) ‘Nato Member Countries’. *Organization, Webpage.* >http://www.nato.int/cps/en/natohq/nato_countries.htm<. [Accessed 21.12.2014].

North Atlantic Treaty Organization (2014c) ‘Search’ *Webpage.* >http://www.nato.int/cps/en/natolive/index.htm<. [Accessed 18.07.2014].

North Atlantic Treaty Organization (2015) ‘Member States’ *web-page.* >http://www.nato.int/cps/en/natohq/topics_52044.htm<. [Accessed 10.02.2015].

O’Malley. Pat (2004) *Risk, Uncertainty and Government.* Routledge-Cavendish. Glass House Press. Oxon. United Kingdom.

O’Malley. Pat (2009) ‘Governmentality and Risk’ *Legal Studies Research Paper 2010 09:98, 1-26.* >http://ssrn.com/abstract=1478289<. [Accessed 04.09.2013].

O’Malley. Pat (2010) ‘Resilient Subjects: Uncertainty, Warfare and Liberalism’ *Economy and Society 2010 39:4, 488-509.* >http://www.tandfonline.com/doi/pdf/10.1080/03085147.2010.510681<. [Accessed 06.09.2013].

O’Malley. Pat (2012) ‘Security after Risk: Security Strategies for Governing Extreme Uncertainty’ *Current Issues in Criminal Justice. 2011-2012 23:5, 5-15,* >http://heinonline.org/HOL/Page?handle=hein.journals/cicj23&div=5&g_sent=1&collection=journals<. [Accessed 05.09.2013].

Oltermann. Philip (2014) ‘Merkel urged to Press Obama on NSA Scandal Ahead of Washington Talks’ *The Guardian. Webpage. 27.04.2014.* >http://www.theguardian.com/world/2014/apr/27/merkel-obama-nsa-scandal-washington-talks<. [Accessed 27.04.2014].

OSCE (2013) ‘Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace’ *Action against Terrorism Unit Transnational Threats Department. Report* > http://www.osce.org/atu/103500<. [Accessed 12.12.2014].

O'Riordan. Tim and Andrew Jordan (1995) ’The Precautionary Principle in Contemporary Environmental Politics’ *Environmental Values 1995 4:3, 191-212.* >http://www.jstor.org/stable/pdfplus/30301451.pdf<. [Accessed 04.09.2013].

Osborne. David and Ted Gaebler (1992) *Reinventing Government: How the Entrepreneur Spirit is Transforming the Public Sector.* Plume. New York. United States.

Owen. Taylor (2004) Human Security-conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-based Definition’ *Security Dialogue 2004 35:3, 373-387.* >http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8

&ved=0CCMQFjAA&url=http%3A%2F%2Fsdi.sagepub.com%2Fcontent%2F35%2F3%2F373.abstract&ei=1HjHVNfiGsL_Uti6gKAO&usg=AFQjCNGu-J3HNGvz7n3hRVY1LhLuL2sm3A&sig2=65I-BINTe2b6rKmVf1ctaA&bvm=bv.84349003,d.d24<. [Accessed 20.12.2014].

Ozdemir. Vural (2009) 'What to do When the Risk Environment is Rapidly Shifting and Heterogeneous? Anticipatory Governance and Real-time Assessment of Social Risks in Multiply Marginalized Populations can Prevent IRB Mission Creep, Ethical Inflation or Underestimation of Risks' *The American Journal of Bioethics 2009 9:1, 65-68.* >http://www.tandfonline.com/doi/full/10.1080/15265160903197671?mobileUi=0#.VMkEUvmzmM8<. [Accessed 21.12.2014].

Paddick. Brian (2014) 'The Surveillance Law is a Threat to Criminals, not Privacy' *The Guardian Commentary. Webpage.* >http://www.theguardian.com/commentisfree/2014/jul/15/surveillance-law-threat-to-criminals-not-privacy< [Accessed 15.07.2014].

Pagliery. Jose (2014) 'Hackers Attack Sony PlayStation Network' *CNN. 24.08.2014. Webpage.* >http://money.cnn.com/2014/08/24/technology/security/sony-playstation-hack/?hpt=hp_t3<. [Accessed 25.08.2014].

Paris. Roland (2001) ''Human Security'. Paradigm Shift or Hot Air?' *International Security 2001 26:2, 87-102.* >http://www.jstor.org/stable/pdfplus/3092123.pdf?acceptTC=true<. [Accessed 03.09.2013].

Paris. Roland, and Timothy D. Sisk (2009) *The Dilemmas of Statebuilding: Confronting the Contradictions of Postwar Peace Operations.* Routledge, Abingdon. United Kingdom.

Patrikakis. Charalampos and Michalis Masikos, and Olga Zouraraki (2004) 'Distributed Denial of Service Attacks' *The Internet Protocol Journal – 2004 7:4. Cisco. Webpage.* >http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html<. [Accessed 20.08.2014].

Pearce. Nick and Martin Weller, Eileen Scanlon & Sam Kinsley (2010) 'Digital Scholarship Considered: How New Technologies Could Transform Academic Work' *In Education 16:1, 33-44.* >http://ineducation.couros.ca/index.php/ineducation/article/view/44/509<. [Accessed 28.08.2014].

Pilkington. Ed (2014) 'LulzSec Hacker 'Sabu' Released after 'Extraordinary' FBI Cooperation' *The Guardian. Webpage. 27.05.2014.* >http://www.theguardian.com/technology/2014/may/27/hacker-sabu-walks-free-sentenced-time-served<. [Accessed 26.05.2014].

Piris. Jean-Claude (2010) *The Lisbon Treaty. A Legal and Political Analysis*. Cambridge University Press. Cambridge. United Kingdom.

Podgor. Ellen. S. (2004) 'Cybercrime: National, Transnational or International?' *Wayne Law Review* 2004 50, 97-109. >http://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/waynlr50&div=13&id=&page=<. [Accessed 10.09.2013].

Poku. Nana K. (2010) 'Globalization, Development, and Security' (Ed.) Collins. Alan. *Contemporary Security Studies*. Oxford University Press. Oxford. United Kingdom.

Pollitt. Mark. M. (1998) 'Cyberterrorism: Fact or Fancy' *Computer Fraud and Security 1998 1998:2, 8-10.* >http://www.sciencedirect.com/science/article/pii/S1361372300870098#<. [Accessed 11.09.2013].

Poulsen. Kevin (2007) '"Cyber-war" and Estonia's Panic Attack' *Wired. 22.08.2007. Threat Level.* >http://www.wired.com/2007/08/cyber-war-and-e/<. [Accessed 23.07.2014].

Pram Gad. Ulrik and Karen Lund Petersen (2011) 'Concepts of Politics in Securitization Studies' *Security Dialogue 2011 42: 4-5,* 315-328. >http://sdi.sagepub.com/content/42/4-5/315.full.pdf+html<. [Accessed 04.09.2013].

Press Association (2014) 'Draft Script for James Bond Film Spectre Leaked in Sony Hack' *The Guardian. 14.12.2014. Webpage.* >http://www.theguardian.com/film/2014/dec/14/james-bond-spectre-film-script-leaked-sony<. [Accessed 20.12.2014].

Provan. Keith G. and Patrick Kenis (2007) 'Modes of Network Governance: Structure, Management and Effectiveness' *Journals of Public Administration Research and* Theory 18: 229-252. >http://jpart.oxfordjournals.org/content/18/2/229.full.pdf<. [Accessed 08.09.2013].

Quay. Ray (2010) 'Anticipatory Governance: A Tool for Climate Change Adaptation' *Journal of the American Planning Association 2010 76:4, 496-*

511. >http://www.tandfonline.com/doi/abs/10.1080/01944363.2010.508428#.VMkIu_mzmM8<. [Accessed 08.01.2015].

Quinn. Ben (2012) ‘Interpol Website Suffers 'Anonymous Cyber-attack’ *The Guardian. 29.02.2012. Webpage.* >http://www.theguardian.com/technology/2012/feb/29/interpol-website-cyber-attack<. [Accessed 27.07.2014].

Radu. Roxana (2013) ‘Power Technology and Powerful Technologies: The Dynamics of Global Governmentality in the Cyberspace’ (Ed.) Kremer. Jan-Frederik and Benedikt Müller (2013) *Cyber Space and International Relations: Theory, Prospects and Challenges*. Springer-Verlag. Berlin. Germany.

Rahman. Rizal (2012) ‘Legal Jurisdiction over Malware-related Crimes: From Theories of Jurisdiction to Solid Practical Application’ *Computer Law and Security Review 2012 28:4, 403-415.* >http://www.sciencedirect.com/science/article/pii/S0267364912000568#<. [Accessed 10.09.2013].

Ransom. John S. (1997) *Foucault’s Discipline: The Politics of Subjectivity*. Duke University Press. Durham. United Kingdom

Ramraj. Victor V. (2007) ’Between Idealism and Pragmatism: Legal and Political Constraints on State Power in Times of Crises’ (Ed.) Goold. Benjamin J. and Liora Lazarus. *Security and Human Rights.* Hart Publishing. Oxford. United Kingdom.

Rasler. Karen and William R. Thompson (2005) *Puzzles of the Democratic Peace: Theory, Geopolitics and the Transformation of World Politics*. Palgrave Macmillan. London. United Kingdom.

Ratnam. Gopal (2012) ‘Cyber Attacks could become as Destructive as 9/11: Panetta’ *Bloomberg Businesses. News from Bloomberg. 12.10.2012. Webpage.* >http://www.bloomberg.com/news/2012-10-12/cyberattacks-could-become-as-destructive-as-9-11-panetta.html<. [Accessed 27.04.2013].

Rehn. Elisabeth (2003) ‘Excessive Reliance on the Use of Force Does Not Stop Terrorism’ (Ed.) Hoeksema. Tammo and Jan Ter Laak (2003) *Human Rights and Terrorism*. NHC/OSCE. Holland.

Reid. Julian (2012) ‘The Disastrous and Politically debased Subject of Resilience’ *Development Dialogue* 2012 58, 67-79. >http://daghammarskjold.hosterspace.com/wp-content/uploads/2012/04/dd58_one_side.pdf#page=67<. [Accessed 28.05.2015].

Renn. Ortwin (2008) *Risk Governance. Coping with Uncertainty in a Complex World*. Earthscan. London. United Kingdom.

Researchomatic (2013) ‘Peoples' Dependence on Computers Technology’ *Retrieved 21.02.2013. Webpage.* >http://www.researchomatic.com/peoples-dependence-on-computers-technology-159370.html<. [Accessed 27.12.2014].

Rid. Thomas (2012) ‘Cyber War Will Not Take Place’ *Journal of Strategic Studies 2012 35:1, 5-32.* >http://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939#.U_ot8vl7zcs<. [Accessed 24.08.2014].

Roberts. David (2006) ‘Review Essay: Human Security or Human Insecurity? Moving the Debate Forward’ *Security Dialogue 2006 37:2, 249-261.* >http://sdi.sagepub.com/content/37/2/249.full.pdf+html<. [Accessed 27.12.2014].

Roe. Paul (2010) ’Societal Security’ (Ed.) Collins. Alan. *Contemporary Security Studies*. Oxford University Press. Oxford. United Kingdom.

Roe. Paul (2012) ‘Is Securitization a 'Negative' Concept? Revisiting the Normative Debate over Normal versus Extraordinary Politics’ *Security Dialogue* 2012 43:3, 249-266. >http://sdi.sagepub.com/content/43/3/249.full.pdf+html<. [Accessed 04.09.2013].

Rose. Nikolas (2001) **’**The Politics of Life Itself’ *Theory, Culture & Society 2001 28:6, 1–30.* >http://tcs.sagepub.com/content/18/6/1.full.pdf<. [Accessed 04.09.2013].

Rose. Nikolas and Peter Mille (1992) ‘Political Power Beyond the State: Problematic of Government’ *The British Journal of Sociology* 1992 43-2, 173-205. >http://www.jstor.org/stable/pdfplus/591464.pdf <. [Accessed 04.02.2011].

Rose. Nikolas, and Pat O’Malley, Mariana Valverde (2006) ‘Governmentality’ *Annual Review of Law and Social Science 2006 2, 83-104.* >http://www.annualreviews.org/doi/abs/10.1146/annurev.lawsocsci.2.081805.105900?journalCode=lawsocsci<. [Accessed 05.09.2013].

Rothschild. Emma (1995) ‘What is Security?’ *Daedalus, The Quest for World Order 1995 124: 3, 53-98.* >http://www.jstor.org/stable/pdfplus/20027310.pdf?acceptTC=true<. [Accessed 28.08.2013].

RT (2013) ‘NATO Launches ‘Largest Ever’ Cyber-security Exercises’ *News. 26.11.2013. Webpage.* >http://rt.com/news/nato-cyber-exercises-estonia-344/<. [Accessed 23.07.2014].

RT (2014) ‘‘Biggest Ever’? Massive DDoS-attack hits EU, US’ *News. 11.02.2014. Webpage.* >http://rt.com/news/biggest-ddos-us-cloudflare-557/<. [Accessed 27.06.2014].

Rudasill. Lynne and Jessica Moyer (2004) ‘Cyber-security, Cyber-attack, and the Development of a Governmental Response: the Librarian’s View’ *New Library Wold 2004 105:7-8, 248-255.* >http://www.emeraldinsight.com/journals.htm?articleid=860190<. [Accessed 09.09.2013].

Rumsfeld. Donald (2002) ‘Press Conference by the US Secretary of Defence’ *NATO Speeches. 06.06.2002. Webpage.* >http://www.nato.int/docu/speech/2002/s020606g.htm<. [Accessed 04.05.2014].

Ryerson. Christie (2010) ‘Critical Voices and Human Security: To Endure, To Engage or To Critique?’ *Security Dialogue 2010 41:2, 169-190.* >http://sdi.sagepub.com/content/41/2/169.full.pdf+html<. [Accessed 03.09.2013].

Sabatier. Paul A. (1986) ‘Top-Down and Bottom-Up Approaches to Implementation Research: A Critical Analysis and Suggested Synthesis’ *Journal of Public Policy 1986 6:1, 21-8.* >http://journals.cambridge.org/action/displayFulltext?type=8&fid=2751860&jid=PUP&volumeId=6&issueId=01&aid=2747728<. [Accessed 31.08.2014].

Salter. Mark. B. (2008a) ’Imaging Numbers: Risk, Quantification, and Aviation Security’ *Security Dialogue 2008 39:2-3, 243-266.* >http://sdi.sagepub.com/content/39/2-3/243.full.pdf<. [Accessed 05.09.2013].

Salter. Mark B. (2008b) ‘Securitization and Desecuritization: A Dramaturgical Analysis of the Canadian Air Transport Security Authority’ *Journal of International Relations and Development 2008 11:4, 321–349.* >http://www.palgrave-journals.com/jird/journal/v11/n4/pdf/jird200820a.pdf<. [Accessed 08.09.2013].

Sandin. Per (1999) ’Dimensions of the Precautionary Principle. Appendix II: Various Formulations of the Precautionary Principle’ *Human and Ecological Risk Assessment: An International Journal, 5: 5, 889-907.* >http://www.tandfonline.com/doi/pdf/10.1080/10807039991289185<. [Accessed 06.09.2013].

Sandin. Per (2004) ’The Precautionary Principle and the Concept of Precaution’ *Environmental Values 2004 13:4, 461-474.* >http://www.jstor.org/stable/pdfplus/30302022.pdf?acceptTC=true<. [Accessed 09.09.2013].

Schaeffer. Peter V. and Scott Loveridge (2002) ‘Towards an Understanding of Types of Public-Private Cooperation’ *Public Performance & Management Review 2002 26:2, 169-189.* >http://www.jstor.org/stable/pdfplus/3381276.pdf?acceptTC=true<. [Accessed 08.09.2013].

Schermer. Bart W. (2011) ‘The Limits of Privacy in Automated Profiling and Data Mining’ *Computer Law & Security Review 2011 27:1, 45-52.*>http://www.sciencedirect.com/science/article/pii/S0267364910001767<. [Accessed 20.12.2014].

Schroeder. Ursula C. (2013) *The Organization of European Security Governance: Internal and External Security in Transition.* Routledge. Abingdon. United Kingdom.

Schmidt, Andreas (2014) ‘Hierarchies in Networks. Emerging Hybrids of Networks and Hierarchies for Producing Internet Security’ (Ed.) Kremer. Jan-Frederik and Benedikt Müller (2014) *Cyber space and international relations: Theory, prospects and challenges*. Springer-Verlag. Berlin. Germany.

Schmitt. Carl (1985) *Political Theory: Four Chapters on the Concept of Sovereignty.* MIT Press. London. United Kingdom.

Schweizer Kirsten (2014) ’Bitcoin Payments by Pedophiles Frustrate Child Porn Fight’ *BloombergBusiness. 10.10.2014. Webpage.* >http://www.bloomberg.com/news/articles/2014-10-09/bitcoin-payments-by-pedophiles-frustrate-child-porn-fight,<. [Accessed 12.01.2015].

Scott. Colin (2000) ‘Accountability in the Regulatory State’ *Journal of Law and Society 2000 27:1, 38-60.* >http://onlinelibrary.wiley.com/doi/10.1111/1467-6478.00146/pdf<. [Accessed 12.01.2015].

Scott. Colin (2001) ‘Analysing Regulatory Space: Fragmented Recourses and Institutional Design’ *Public Law* 2001 *329-353.* >http://login.westlaw.co.uk/maf/wluk/app/document?&src=ri&docguid=ID116A470E72111DA9D198AF4F85CA028&hitguid=ID116A470E72111DA9D198AF4F85CA028&srguid=ia744d065000001411d90367e9cd03d51&spos=1&epos=1&td=1&refer=%2Fmaf%2Fwluk%2Fapp%2Fdocument%3Fspos%3D1%26ran

k%3D1%26hitguid%3DID116A470E72111DA9D198AF4F85CA028%26docguid%3DIE00CC8A0E7131 1DA915EF37CAC72F838%26resolvein%3Dtrue%26crumb-action%3Dappend%26td%3D1%26suppsrguid%3Dia744d065000001411d90367e9cd03d51%26epos%3D1 %26context%3D14&crumb-action=append&context=15<. [Accessed 12.09.2013].

Scott. Colin (2002) 'Private Regulation of the Public Sector: A Neglected Facet of Contemporary Governance' *Journal of Law and Society 2002 29:1, 56-76.* >http://www.jstor.org/stable/pdfplus/4489081.pdf<. [Accessed 08.09.2013].

Scott. Colin and Fabrizio Cafaggi, Linda Senden (2011) 'The Conceptual and Constitutional Challenge of Transnational Private Regulation' Journal of Law and Society 2011 38:1, 1-19. >http://onlinelibrary.wiley.com/doi/10.1111/j.1467-6478.2011.00532.x/pdf<. [Accessed 20.08.2014].

Seddon. Toby (2010) 'Rethinking Prison Inspection' (Ed.) Hannah Quirk, Toby Seddon, Graham Smith (2010) *Regulation and Criminal Justice: Innovations in Policy and Research*. Cambridge University Press. Cambridge. United Kingdom.

Shackelford. Scott J. (2014) *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace.* Cambridge University Press. Cambridge. United Kingdom, Preface, XIX.

Shah. Sooraj (2014) 'Evernote Latest to be Struck by DDoS Attack' *Computing. 11.06.2014. Webpage.* >http://www.computing.co.uk/ctg/news/2349431/evernote-latest-to-be-struck-by-ddos-attack<. Accessed 27.-7.2014].

Shearing. Clifford (2006) 'Reflections on the Refusal to Acknowledge Private Governments' (Ed.) Wood. Jennifer and Benoît Dupont. *Democracy, Society and the Governance of Security.* Cambridge University Press. Cambridge. United Kingdom.

Sheehan. Michael (2005) *International Security. An Analytical Survey.* Lynne Rienner Publishers. London. United Kingdom.

Sheehan. Michael (2010) 'Military Security' (Ed.) Collins. Alan. *Contemporary Security Studies.* Oxford University Press. Oxford. United Kingdom.

Shontell. Alyson (2014) 'Apple Statement on Celebrity Hacking: Our Systems Weren't Breached' *Business Insider, 02.09.2014. Webpage.* >http://www.businessinsider.com/apple-statement-on-celebrity-hacking-2014-9?IR=T< . [Accessed 12.01.2015].

Siddique. Haroon (2014) 'Jihadi Recruitment Video for Islamist Terror Group Isis Features three Britons' *The Guardian. 21.06.2014. Webpage.* >http://www.theguardian.com/world/2014/jun/20/jihadi-recruitment-video-islamist-terror-group-isis-features-britons<. [Accessed 20.07.2014]. Kingsley. Patrick (2014)

Silomon. Jantje A.M. and Richard E. Overill (2012) 'Cybersecurity's Can of Worms' *Journal of Information Warfare 2012 11, 1: 12 – 21.* >http://scholar.google.co.uk/scholar?q=Silomon.+Jantje+A.M.+and++Richard+E.+Overill+%282012%29+%E2%80%98Cybersecurity%E2%80%99s+Can+of+Worms%E2%80%99.+Journal+of+Information+Warfare+2012+11%2C+1%3A+12+%E2%80%93+21%2C+12.&btnG=&hl=en&as_sdt=0%2C5<. [Accessed 10.10.2014].

Simon. Jonathan (2008) 'Choosing our Wars, Transforming Governance. Cancer, Crime, and Terror' (Ed.) Louise Amoore and Marieke de Goede. *Risk and the War on Terror.* Routledge. Abingdon. United Kingdom.

Sinclair-Webb. Emma (2014) 'Dispatches: Turkey Shuts Down Twitter' *Human Right Watch. Webpage.* 21.03.2014. >http://www.hrw.org/news/2014/03/21/dispatches-turkey-shuts-down-twitter<. [Accessed 20.04.2014*]*.

Singer. Peter Warren (2003) *Corporate Warriors: The Rise of the Privatized Military Industry*. Cornell University Press. Ithaca. United States.

Sjöberg. Lennart and Bjørn-Elin Moer, Thorbjørn Rundmo (2004) *Explaining Risk Perception. An Evaluation of the Psychometric Paradigm in Risk Perception Research*. Rotunde Publikasjoner. Trondheim. Norway. >http://www.svt.ntnu.no/psy/Torbjorn.Rundmo/Psychometric_paradigm.pdf<. [Accessed 02.09.2013].

Sky News (2012) 'HSBC Suffers 'Large Scale' Cyber Attack' *Technology. 19.10.2012. Webpage.* >http://news.sky.com/story/999914/hsbc-suffers-large-scale-cyber-attack<. [Accessed 12.09.2013].

Slaughter, Anne-Marie (2004) *A New World Order* Princeton University Press. Princeton. United States.

Slovic. Paul and Elke U. Weber (2002) ‘Perception of Risk Posed by Extreme Events’ *Unpublished Paper. Presented at “Risk Management Strategies in an Uncertain World” Conference. Palisades. New York. April 12-13 2002.* >http://cursos.campusvirtualsp.org/pluginfile.php/7062/mod_page/content/1/modulo2/content/perception-of-risk-posed-by-extreme-events.pdf<. [Accessed 06.09.2013].

Smismans. Stjin (2005) ‘Reflexive Law in Support of Directly Deliberative Polyarchy: Reflexive-deliberative Polyarchy as a Normative Frame for the OMC’ (Ed.) De Schutter. Olivier and Simon Deakin. *Social Rights and Market Forces: Is the Open Coordination of Employment and Social Policies the Future of Social Europe?* Bruylant. Brussels. Belgium.

Smith. Graham (2009) ‘Citizens Oversight of Independent Police Services: Bifurcated Accountability, Regulation Creep and Lesson-Learning’ *Regulation and Governance 2009 3:4, 422-442.* >http://www.readcube.com/articles/10.1111/j.1748-5991.2009.01061.x<. [Accessed 20.12.2014].

Smith. Rhonda K. M. (2007) *Textbook on International Human Rights*. Oxford University Press. Oxford. United Kingdom.

Snow. Nancy (2014) ‘Isis Beheading Videos: The Scariest Part is how Well their Propaganda is Working’ *The Guardian. 03.09.2014. Webpage.* >http://www.theguardian.com/commentisfree/2014/sep/03/isis-beheading-videos-propaganda-working<. [Accessed 04.09.2014].

Sofaer. Abraham D. (2003) ‘On the Necessity of Pre-emption’ *European Journal of International Law. 2003 14:2, 209-226.* >http://ejil.oxfordjournals.org/content/14/2/209.full.pdf<. [Accessed 07.09.2013].

Sommestad. Teodor and Jonas Hallberg (2012) ‘Cyber Security Exercises and Competitions as a Platform for Cyber Security Experiments’ *Secure IT Systems Lecture Notes in Computer Science 2012 7617, 47-60, 47.* >http://link.springer.com/chapter/10.1007%2F978-3-642-34210-3_4#<. [Accessed 13.01.2015].

Steele. Jenny (2004) *Risk and Legal Theory*. Hart Publishing. Oxford. United Kingdom.

Spitters. Martijn and Stefan Verbruggen, Mark van Staalduinen (2014) ‘Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services’ *Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint, 2014 220-223.*>http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6975577<. [Accessed 20.12.2014].

Stern. Jessica and Jonathan B. Wiener (2006) ‘Precaution against Terrorism’ *Journal of Risk Research 2006 9:4, 393-447.* >http://www.tandfonline.com/doi/pdf/10.1080/13669870600715750<. [Accessed 07.09.2013].

Strate. Lance (1999) ’The Varieties of Cyberspace: Problems in Definition and Delimitation’ *Western Journal of Communication 1999 63:3, 382-412.>* http://www.tandfonline.com/doi/abs/10.1080/10570319909374648#.VMZQOfmzmM8<. [Accesed 17.12.2014].

Strauss, Anslem (1987) Qualitative analysis for social scientists. Cambridge University Press. Cambridge. United Kingdom.

Strauss and Corbin (1990) *Basics of qualitative research: Grounded theory procedures and techniques.* Sage Publications. Thousand Oaks. United States.

Stritzel. Holger (2007) ‘Towards a Theory of Securitization: Copenhagen and Beyond’ *European Journal of International Relations 2007 13:3, 357-383.* >http://ejt.sagepub.com/content/13/3/357.full.pdf<. [Accessed 07.09.2013].

Sunstein. Cass R. (2003) ’Beyond the Precautionary Principle’ *University of Pennsylvania Law Review 2003 151:3, 1003-1058.* >http://www.jstor.org/stable/pdfplus/3312884.pdf?acceptTC=true<. [Accessed 06.09.2013].

Sunstein. Cass R. (2005) *Laws of Fear. Beyond the Precautionary Principle*. Cambridge University Press. Cambridge. United Kingdom.

Sunstein. Cass R. (2008) ‘Irreversibility’ *Law, Probability and Risk 2010 9, 227−245.* >http://lpr.oxfordjournals.org/content/9/3-4/227.full.pdf+html<. [Accessed 06.09.2013].

Svantesson. Dan and Roger Clarke (2010) ‘Privacy and Consumer Risks in Cloud Computing’ *Computer Law & Security Review 2010 26:4, 391-397.* >http://www.sciencedirect.com/science/article/pii/S0267364910000828<. [Accessed 23.11.2014].

Tadros. Victor (2007) 'Justice and Terrorism' *New Criminal Law Review: An International and Interdisciplinary Journal 2007 10:4, 658-689.* >http://www.jstor.org/stable/pdfplus/10.1525/nclr.2007.10.4.658.pdf?&acceptTC=true&jpdConfirm=true<. [Accessed 09.09.2013].

Tait. Joyce and Ann Bruce (2004), 'Global Change and Transboundary Risks' (Ed.) McDaniels. Timothy and Mitchell Small (2004) *Risk Analysis and Society: an Interdisciplinary Characterisation of the Field,* Cambridge University Press. Cambridge. United Kingdom (Commissioned by Society for Risk Analysis for the International Symposium on Risk and Governance, Warrenton, VA, USA, June 2000).

Tait. Joyce and Chataway, Joanna, David Wield (2004) 'Governance, Policy and Industry Strategies: Agro-biotechnology and Pharmaceuticals', *Innogen Working Paper 12.* >http://www.innogen.ac.uk/ownPubs/Innogen_paper_12.pdf.<. [Accessed 22.12.2014].

Taureck. Rita (2006) 'Securitization theory and Securitization Studies' *Journal of International Relations and Development 2006 9:1, 53-61.*> http://www.palgrave-journals.com/jird/journal/v9/n1/pdf/1800072a.pdf<. [Accessed 09.01.2015].

Taylor. John B. (2007) *Global Financial Warriors: The Untold Story of International Finance in the Post-9/11 World*. W. W. Norton. New York. United States.

Taylor. Stephanie (2001) 'Locating and Conducting Discourse Analytic Research' (Ed.) Wetherell. Margaret and Stephanie Taylor, Simeon J Yates (2001) *Discourse as Data: A Guide for Analysis*. Open University. Milton Keynes. United Kingdom.

Tekofsky. A. (2006) 'Security in European External Border Law' *CHALLENGE Working Paper WP13 19.* >http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=3&cad=rja&uact=8&ved=0CDEQFjAC&url=http%3A%2F%2Fwww.libertysecurity.org%2FIMG%2Fpdf%2FState_of_the_Art.pdf&ei=BD-LVPeHGouqUaibhPAN&usg=AFQjCNHmpwXAUHAV3Yp82CTcpCHzTtnW7Q&sig2=7kG6gcwpyJ2NXqQqHrV3_w<. [Accessed 26.12.2014].

Terriff. Terry and Stuart Croft, Lucy James, Patrick M. Morgan (1999) *Security Studies Today*. Polity Press. Cambridge. United Kingdom.

The Economist (2014a) 'Defending the digital frontier' *Special report: Cyber-security, 12.07.2014, Webpage.* >http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals?frsc=dg%7ca<. [Accessed 17.07.2014].

The Economist (2014b) 'Hackers Inc. Cyber-attackers have Multiplied and Become far more Professional' *Special Report: Cybercrime. 12.07.2014. Webpage.* >http://www.economist.com/news/special-report/21606421-cyber-attackers-have-multiplied-and-become-far-more-professional-hackers-inc?frsc=dg%7ca<. [Accessed 21.07.2014].

The Guardian (2007) 'Russia Accused of Unleashing Cyberwar to Disable Estonia' *News. 17.05.2007. Webpage.* >http://www.guardian.co.uk/world/2007/may/17/topstories3.russia<. [Accessed 09.09.2013].

The Guardian (2013/2014) 'The NSA Files. How the Story Unfold' *The Guardian. Web-portal.* >http://www.theguardian.com/world/the-nsa-files<. [Accessed 04.09.2014].

The Guardian (2014a) 'Cyber-attacks on South Korean Nuclear Power Operator Continue'. *28.12.2014. Webpage.* >http://www.theguardian.com/world/2014/dec/28/cyber-attacks-south-korean-nuclear-power-operator<. [Accessed 31.12.2014].

The Guardian (2014b) 'The Issues, The Oversight' *The NSA Files. Webpage.* >http://www.theguardian.com/world/the-nsa-files<. [Accessed 06.07.2014].

The Guardian (2014c) 'Turkish Police Crack Down on Internet Freedom Protest' *09.02.2014. Webpage.* >http://www.theguardian.com/world/2014/feb/09/turkish-police-crack-down-on-internet-freedom-protest<. [Accessed 23.04.2014].

The International Telecommunication Union (2014) 'Definition of Cybersecurity' *Standardization Webpage.* >http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx< [Accessed 20.03.2014].

The Mentor (1986) The Conscience of a Hacker (Hacker's Manifesto). *Darknet.org.uk. Webpage.* >http://www.darknet.org.uk/2010/04/the-conscience-of-a-hacker-aka-the-hackers-manifesto-by-the-mentor/<. [Accessed 12.12.2014].

The Telegraph (2014) ‘Nato Websites Targeted in Cyber Attack over Crimea Stance’ *Reuters. 16.03.2014. Webpage.* >http://www.telegraph.co.uk/news/worldnews/europe/ukraine/10700861/Nato-websites-targeted-in-cyber-attack-over-Crimea-stance.html<. [Accessed 20.07.2014].

Thomas. Caroline (2000) *Global Governance, Development and Human Security: The Challenge of Poverty and Inequality.* Pluto. London. United Kingdom.

Thomas. Nicholas, and William T. Tow (2002) ‘The Utility of Human Security: Sovereignty and Humanitarian Intervention’ *Security Dialogue 2002 33:2, 177-192.* >http://sdi.sagepub.com/content/33/2/177.full.pdf+html<. [Accessed 23.11.2014].

Tombs. Steve and David Whyte (2006) ‘Work and Risk’ (Ed.) Mythen, Gabe and Sandra Walklate (2006) *Beyond the Risk Society*. McGraw Hill. London. United Kingdom.

Thompson. Dennis F. (1980) ‘Moral Responsibility of Public Officials: The Problem of Many Hands’ *American Political Science Review 74, 905-916.* >http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=8942769&fileId=S0003055400169515<. [Accessed 20.12.2014].

Tikk. Eneken (2011) ‘Ten Rules for Cyber Security‘ *Survival: Global Politics and Strategy 2011 53:3, 119-132.* >http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.571016#.UeG5q_l7zcs<. [Accessed 09.09.2013].

Tikk. Eneken and Kadri Kaska, Liis Vihul (2010) ’International Cyber Incidents: Legal Considerations’ *Cooperative Cyber Defence Centre of Excellence (CCD COE) Report.* >www.ccdcoe.org/publications/books/legalconsiderations.pdf<. [Accessed 09.09.2013].

Tran. Mark (2014) ‘Who are Isis? A Terror Group too Extreme even for al-Qaida’ *The Guardian. 11.06.2014. Webpage.* >http://www.theguardian.com/world/2014/jun/11/isis-too-extreme-al-qaida-terror-jihadi<. [Accessed 17.07.2014].

Tran. Mark and Matthew Weaver (2014) ‘Isis Announces Islamic Caliphate in Area Straddling Iraq and Syria’ The Guardian. >http://www.theguardian.com/world/2014/jun/30/isis-announces-islamic-caliphate-iraq-syria<. [Accessed 05.02.2015].

Travis. Alan (2014) ‘Counter-terrorism and Security Bill: Proposals and Pitfalls’ *The Guardian. 24.11.2014. Webpage.* >http://www.theguardian.com/uk-news/2014/nov/24/counter-terrorism-security-bill-proposals-pitfalls<. [Accessed 15.07.2014].

Travis. Alan and Charles Arthur (2014) ‘EU Court Backs ‘Right to be Forgotten’: Google must Amend Results on Request’ *The Guardian, Technology. Webpage.* >http://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results<. [Accessed 15.07.2014].

Towel. Philip (2005) ‘Cold War’ (Ed.) Townshend. Charles. *The Oxford History of Modern War.* Oxford University Press. Oxford. United Kingdom.

Tsoukala. Anastassia (2004) ‘Democracy against Security: The Debates about Counter-Terrorism in the European Parliament, September 2001- June 2003’ *Alternatives: Global, Local, Political 2004 29:4, 417-439.* >http://alt.sagepub.com/content/29/4/417.full.pdf+html<. [Accessed 04.09.2013].

Tsoukas. Haridimos (1989) ‘The Validity of Idiographic Research Explanations’*Academy of Management Review 189 14:4, 551-61.* > http://amr.aom.org/content/14/4/551.full.<. [Accessed 05.10.2014].

Uda. Robert. T. (2009) ‘Cybercrime, Cyberterrorism, and Cyberwarfare in Perspectives’ (Ed.) Uda. Robert T. *Cybercrime, Cyberterrorism, and Cyberwarfare. Crime, Terror and War without Conventional Weapons.* Xlibris Corporation. United States.

UK.Gov (2011) *The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World.* >https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. [Accessed 08.09.2013].

Ullman. Richard H. (1983) ‘Redefining Security’ *International Security 8:1, 129-133.* >http://www.jstor.org/stable/pdfplus/2538489.pdf <. [Accessed 03.09.2013].

United Nations (1945a) ‘Charter of the United Nation and the Statute of the International Court of Justice’. *Charter of the United Nations.* >http://www.un.org/en/documents/charter/index.shtml<. [Accessed 09.09.2013].

United Nations (1994) ‘United Nations Declaration on Measures to Eliminate International Terrorism Annex to UN General Assembly Resolution 49/60’ *General Assembly. UN Doc. A/Res/60/49.* >http://www.un.org/documents/ga/res/49/a49r060.htm<. [Accessed 10.09.2013].

United Nations (2004a) ‘Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures’ *General Assembly. Resolution 58/199. A/ES/58/199.* >http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf<. [Accessed 09.09.2013].

United Nations (2004b) ‘United Nations Convention against Transnational Organized Crime’ *United Nations on Drugs and Crime A/RES/55/25.* >http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf<. [Accessed 09.09.2013].

United Nations (2004c) ‘Threats to International Peace and Security Caused by Terrorist Acts’ *UN Security Council Resolution 1566 S/RES/1566 (2004).* >http://daccess-ods.un.org/TMP/4029936.19441986.html<. [Accessed 10.09.2013].

United Nations Development Programme (1994) *Human Development Report*. Oxford University Press. New York. >http://hdr.undp.org/en/media/hdr_1994_en_contents.pdf<. [Accessed 03.09.2013].

United Nations Environmental Programme (1992) ‘Principle 15’ *Rio Declaration on Environment and Development*. >http://www.unep.org/Documents.Multilingual/Default.asp?documentid=78&articleid=1163<. [Accessed 05.09.2013].

University of Sheffield (2015) ‘What is Discourse Analysis?’ *Branches of Linguistics. Webpage.* >https://sites.google.com/a/sheffield.ac.uk/all-about-linguistics/branches/discourse-analysis/what-is-discourse-analysis<. [Accessed 04.01.2015].

Vaidyanathan. Rajini (2012) ‘Hacking Group Anonymous takes on India Internet ‘Censorship’’. *News. 09.06.2012. Webpage.* >http://www.bbc.co.uk/news/technology-18371297<. [Accessed 26.07.2014].

Valverde. Mariana (2002**)** ‘Governing Security, Governing through Security’ (Ed.) Daniels. Ronald and Patrick Macklem, Kent Roach, *The Security of Freedom: Essays on Canada’s Anti-terrorism Bill.* University of Toronto Press. Toronto. Canada.

Van Munster. Rens (2005) ‘Logics of Security: The Copenhagen School, Risk Management and the War on Terror’ *Political Science Publications* 10/2005. >http://static.sdu.dk/mediafiles//Files/Om_SDU/Institutter/Statskundskab/Skriftserie/05RVM10.pdf<. [Accessed 29.08.2013].

Van Munster. Rens (2007) ‘Review Essay: Security on a Shoestring: A Hitchhiker’s Guide to Critical Schools of Security in Europe’ *Cooperation and Conflict* 2007 42:2, 235-243. >http://cac.sagepub.com/content/42/2/235.short<. [Accessed 04.09.2013].

Vedby Rasmussen. Mikkel (2001) ‘Reflexive Security: NATO and International Risk Society’ *Millennium – Journal of International Studies* 2001 30:2, 285-309. >http://mil.sagepub.com/content/30/2/285.full.pdf <. [Accessed 03.09.2013].

Vedby Rasmussen. Mikkel (2002) ‘‘A Parallel Globalization of Terror’: 9-11. Security and Globalization’ *Cooperation and Conflict* 2002 37:3, 323-349. >http://cac.sagepub.com/content/37/3/323.full.pdf<. [Accessed 08.09.2013].

Vedby Rasmussen. Mikkel (2004) ‘’It Sounds Like a Riddle’: Security Studies, the War on Terror and Risk’ *Millennium - Journal of International Studies* 2004 33:2, 381-396. >http://mil.sagepub.com/content/33/2/381.full.pdf+html<. [Accessed 03.09.2013].

Vedby Rasmussen. Mikkel (2006) *The Risk Society at War. Terror, Technology and Strategy in the Twenty-first Century.* Cambridge University Press. Cambridge. United Kingdom.

Von Clausewitz. Carl (1997) *On War.* Reprint. Wordsworth Editions. Ware. United Kingdom.

Waddington. P.A.J. (2005) ‘Slippery Slopes and Civil Libertarian Pessimism’ *Policing and Society 15:3, 353-375.* >http://www.tandfonline.com/doi/abs/10.1080/13557850500169204#.VCVt6fldVqU<. [Accessed 20.08.2014].

Waddington. P.A.J. (2006) ‘Terrorism and Civil Libertarian Pessimism: Continuing the Debate’ *Policing and Society 2006 16:4, 415-421.* >http://www.tandfonline.com/doi/full/10.1080/10439460600973750#.VCVuavldVqU<. [20.08.2014].

Waldron. Jeremey (2003) ‘Security and Liberty: The Image of Balance’ *The Journal of Political Philosophy 2003 11:2, 191–210*. >https://apps.osgoode.yorku.ca/Quickplace/peerzumbansen/PageLibrary85256F640073DD82.nsf/0/1244328D995779CD85256F640077236E/$file/Waldron%20Security%20and%20Liberty.pdf<.

Walker. Clive (2007) ‘The Treatment of Foreign Terror Suspects’ *Modern Law Review 2007 70:3, 427-457.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2230.2007.00645.x/pdf<. [Accessed 09.09.2013].

Walker. Peter (2014) ‘North Korea Threatens US, Claiming White House was Involved in Film Plot’ *The Guardian. 22.12.2014. Webpage*. >http://www.theguardian.com/world/2014/dec/22/north-korea-threatens-target-white-house-obama-sony-hacking<. [Accessed 0901.2015].

Walker. Jeremy and Melinda Cooper (2011) ‘Genealogies of Resilience from Systems Ecology to the Political Economy of Crisis Adaptation’ *Security dialogue* 2011 42:2, 143-160. >http://sdi.sagepub.com/content/42/2/143.short<. [Accessed 28.05.2015].

Walklate. Sandra and Ross McGarry, Gabe Mythen (2013) ‘Searching for Resilience: An Conceptual Excavation’ *Armed Forces & Society* 2013 1-20, >http://afs.sagepub.com/content/early/2013/01/29/0095327X12465419.full.pdf+html<. [Accessed 06.09.2013].

Walklate. Sandra and Gabe Mythen, Ross McGarry (2013b) ‘States of Resilience and the Resilient State’ *Current Issues Crim. Just.* 2012 24,185. >http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/cicj24&section=20<. [Accessed 28.05.2015].

Wall. David S. (1998). ‘Catching Cybercriminals: Policing the Internet’ *International Review of Law, Computers & Technology, 12:2, 201-218.* >http://www.tandfonline.com/doi/abs/10.1080/13600869855397<. [Accessed 20.12.2014].

Wall. David S. (2003) *Crime and the Internet*. Routledge. Abingdon. United Kingdom.

Wall. David S. (2007a) *Cybercrime: The Transformation of Crime in the Information Age.* Polity Press. Cambridge. United Kingdom.

Wall. David S. (2007b) ‘Policing Cybercrimes: Situating the Public Police in Networks of Security within the Cyberspace’ *Police Practice and Research. An International Journal 2007 8:2, 183-205.* >http://papers.ssrn.com/sol3/papers.cfm?abstract_id=853225<. [Accessed 10.09.2013].

Wall. David S. (2010) ‘The Internet as a Conduit for Criminal Activity’ (Ed.) Pattavina. A. (2010) *Information Technology and The Criminal Justice System.* >http://papers.ssrn.com/sol3/papers.cfm?abstract_id=740626<. [Accessed 17.12.2014].

Walt. Stephen M. (1991) ‘The renaissance of security studies’ *International Studies Quarterly 35:2,211-239*. >http://www.jstor.org/stable/2600471?seq=1#page_scan_tab_contents<. [Accessed 05.02.2014].

Waltzer. Michael (1977) *Just and Unjust War. A Moral Argument with Historical Illustrations*. Basic Books. New York. United States.

Wark. McKenzie (2004) ‘Hacker’s Manifest Version 2.0. Academia.edu. >http://www.academia.edu/182789/A_Hacker_Manifesto<. [Accessed 12.01.2015].

Wark. McKenzie (2006) ‘Hackers’ *Theory, Culture & Society 2006 23: 2-3, 320-322.* >http://tcs.sagepub.com/content/23/2-3/320.short<. [Accessed 28.08.2014].

Watt. Nicholas (2014) ‘‘Dark Web’: GCHQ and National Crime Agency Join Forces in Hunt for Child Abuse’ *The Guardian. 12.12.2014.* >http://www.theguardian.com/society/2014/dec/11/gchq-national-crime-agency-dark-web-child-abuse<.

Webber. Mark and Stuart Croft, Jolyon Howorth, Terry Terriff and Elke Krahmann (2004) ‘The Governance of European Security’ *Review of International Studies, 2004 30:1, 3-26.* >http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=188601&fileId=S0260210504005807<. [Accessed 28.08.2014].

Weber. Rolf H. (2010) ‘Internet of Things–New Security and Privacy Challenges’ *Computer Law & Security Review 2010 26:1, 23-30.* > http://www.sciencedirect.com/science/article/pii/S0267364909001939<. [Accessed 18.12.2014].

Weimann. Gabriel (2005) Cyber-terrorism: The Sum of All Fears? *Studies in Conflict & Terrorism,* 2005 28:129–149

>http://www.ingentaconnect.com/content/routledg/uter/2005/00000028/00000002/art00004<.[Accessed 18.12.2014].

Weiss. Thomas G. and Danielle Zach Kalbacher (2008) 'The United Nations' (Ed.) Collins. Alan (2008) *Contemporary Security Studies.* Oxford University Press. Oxford. United Kingdom.

Wibben. Annick T.R. (2008) 'Human Security: Towards an Opening' *Security Dialogue 2008 39:4, 445-462.* >http://sdi.sagepub.com/content/39/4/455.full.pdf+html<. [Accessed 03.09.2013].

Wibben. Annick T.R. (2010) *Feminist Security Studies: A Narrative approach*. Routledge, Abingdon. United Kingdom.

Wilkinson. Iain (2009) Risk, Vulnerability and Everyday Life, Routledge, London. United Kingdom.

Wilkinson. Paul (2011) *Terrorism versus Democracy. The Liberal State Response*. Routledge. Abingdon. United Kingdom.

Williams. Dan (2014) 'Israel Tests Arrow Missile Shield, sees Hezbollah Threat' *Reuters. Jerusalem. Webpage.* >http://www.reuters.com/article/2014/01/03/us-arms-israel-arrow-idUSBREA020E120140103<. [Accessed 13.08.2014].

Williams. Matthew (2007) 'Policing and Cybersociety: The Maturation of Regulation within an Online Community' *Policing and Society, 17: 1, 59-82.* >http://www.tandfonline.com/doi/pdf/10.1080/10439460601124858<. [Accessed 09.09.2013].

Williams. Michael. J. (2008) '(In)Security Studies, Reflexive Moderniziation and the Risk Society' *Cooperation and Conflicts 2008 43:1, 57-79.* >http://cac.sagepub.com/content/43/1/57.full.pdf<. [Accessed 05.09.2013].

Williams. Paul. D. (2008) 'Introduction' (Ed.) Williams. Paul D. *Security Studies: An Introduction.* Routledge. Oxon. United Kingdom.

Wirtz, James J. (2010) 'Weapons of Mass Destruction' (Ed.) Collins, Alan (2010) *Contemporary Security Studies*. Oxford University Press. Oxford. United Kingdom.

Wingspread Conference (1998) *Wingspread Statement on the Precautionary Principle*. Racine, Wisconsin, United States. >http://www.rewi.uni-jena.de/rewimedia/Downloads/LS_Ruffert/Ethical+Codes/Wingspread+Conference_Wingspread+Statement+on+the+Precautionary+Principle.pdf<. [Accessed 09.09.2013].

Wintour. Patrick (2014) 'Emergency Surveillance Law to be Brought in with Cross-party Support' *The Guardian 10.06.2014. Webpage.* >http://www.theguardian.com/technology/2014/jul/10/emergency-surveillance-laws-rushed-through-cross-party-support<. [Access 15.07.2014].

Wintour. Patrick Rowena Mason and James Ball (2014) 'David Cameron makes Concessions to Rush through Snooping Law' *The Guardian 10.06.2014. Webpage.* >http://www.theguardian.com/world/2014/jul/10/david-cameron-concessions-snooping-law-surveillance<. [Accessed 15.07.2014].

Wolfers. Arnold (1962) ''National Security' as an Ambiguous Symbol' *Political Science Quarterly 1962 67:4, 481-502.* >http://links.jstor.org/sici?sici=0032-3195%28195212%2967%3A4%3C481%3A%22SAAAS%3E2.0.CO%3B2-R<. [Accessed 17.12.2014].

Wong. Rebecca (2011) 'Data Protection: The Future of Privacy' *Computer Law & Security Review 2011 27:1, 53-57.* >http://www.sciencedirect.com/science/article/pii/S0267364910001718<. [Accessed 17.12.2014].

Wood. Jennifer and Benoit Dupont (2006) 'Introduction' (Ed) Wood. Jennifer and Benoit Dupont. *Democracy, Society and the Governance of Security.* Cambridge University Press. Cambridge. United Kingdom.

Wood. Jennifer and Clifford Shearing (2007) *Imagining Security*. Willan Publishing. Cullompton. United Kingdom**.**

Wæver. Ole (2004) 'Aberystwyth, Paris, Copenhagen. New Schools in Security Theory and their Origins between Core and Periphery' *Unpublished Paper. Paper Presented at an Annual Meeting of the International Studies Association. Montreal. March 17-20, 2004.* >http://www.constructivismointegracion.wikispaces.com<. [Accessed 30.11.2009].

Wæver. Ole (2011) 'Politics, Security, Theory' *Security Dialogue* 2011 42:4-5, 465-480 >http://sdi.sagepub.com/content/42/4-5/465.full.pdf+html<. [Accessed 09.09.2013].

Yar. Majid (2005a) 'Computer hacking: Just another case of juvenile delinquency?' *The Howard Journal of Criminal Justice 2005 44:4, 387-399.* > http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2311.2005.00383.x/abstract<. [Accessed 20.12.2014].

Yar. Majid (2005b) 'The Novelty of 'Cybercrime' an Assessment in Light of Routine Activity Theory' *European Journal of Criminology, 2:4, 407-427.* > http://euc.sagepub.com/content/2/4/407.short<. [Accessed 16.12.2014].

Yar. Majid (2006) *Cybercrime and Society*. Sage Publications. London. United Kingdom.

Yeung. Henry Wai-Chung (1998) 'Capital, State and Space: Contesting the Borderless World' *Transactions of the Institute of British Geographers 1998 (2004) 23:3, 291-309.* >http://onlinelibrary.wiley.com/doi/10.1111/j.0020-2754.1998.00291.x/pdf<. [Accessed 08.09.2013].

Yin. Robert K. (2014) *Case Study Research: Design and Methods*. Sage Publications. California.

Young. Karan (2008) 'Towards an Understanding of Regulation by Design (Ed.) Brownswood. Roger and Karen Yeung. *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*. Hart Publishing. Oxford. United Kingdom.

Zedalis. Rex J. (2005) 'Circumstances Justifying Pre-emptive Self-defence: Thoughts Prompted by the Military Action against Iraq' *Nordic Journal of International Law 74:2, 209-230.* >http://docserver.ingentaconnect.com/deliver/connect/mnp/09027351/v74n2/s2.pdf?<. [Accessed 07.09.2013].

Zedner. Lucia. (2005). 'Securing Liberty in the Face of Terror: Reflections from Criminal Justice' *Journal of Law and Society 2005 32:4, 507-53.* >http://onlinelibrary.wiley.com/doi/10.1111/j.1467-6478.2005.00336.x/full<. [Accessed 15.12.2014].

Zedner. Lucia (2007) 'Seeking Security by Eroding Rights: The Side-stepping of Due Process' (Ed.) Goold. Benjamin J. and Liora Lazarus. *Security and Human Rights*. Hart Publishing. Portland. United States.

Zedner. Lucia (2009) *Security.* Routledge. Abingdon. United Kingdom.

Zetter. Kim (2014) 'Sony Go So Far' *Wired. 03.12.2014. Webpage.* >http://www.wired.com/2014/12/sony-hack-what-we-know t Hacked Hard: What We Know and Don't Know/<. [Accessed 10.12.2014].

Zinn. Jens. O. (2008a) 'A Comparison of Sociological Theorizing on Risk and Uncertainty' (Ed.) Zinn. Jens O. *Social Theories of Risk and Uncertainty. An Introduction.* Blackwell Publishing. Oxford. The United Kingdom.

Zinn. Jens O. (2008b) 'Glossary' (Ed.) Zinn. Jens O. *Social Theories of Risk and Uncertainty. An Introduction.* Blackwell Publishing. Oxford. United Kingdom.

Zittrain. Jonathan (2008) 'Perfect Enforcement' (Ed.) Brownswood. Roger and Karen Yeung. *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*. Hart Publishing. Oxford. United Kingdom.

9 Appendix

9.1 Appendix 1: The European Region

The European Region

The criterion: The country is placed in the geographical region of Europe AND is member of one or more of the three main security institutions: NATO, CoE and EU.

North-Atlantic Treaty Organization (2015):

Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, the United Kingdom and the United States, Greece and Turkey, Germany, Spain, the Czech Republic, Hungary and Poland, Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia, Slovenia, and Albania and Croatia.[881]

The Council of Europe (2015):

Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Macedonia’ Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom.

The European Union (2015):

Member states of the EU: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece , Hungary, Ireland , Italy, Latvia , Lithuania , Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom .[882]

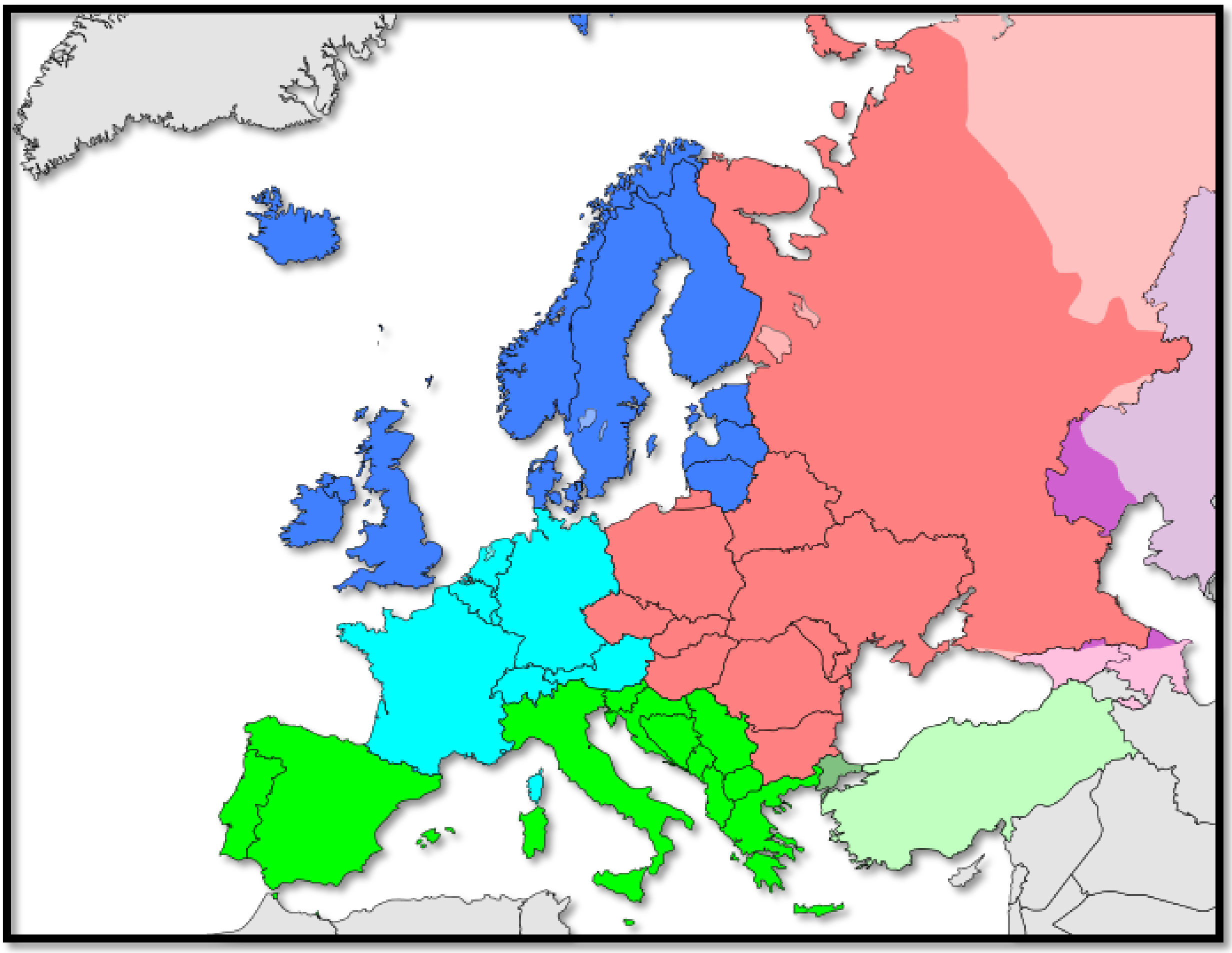
Geographical sphere information provided by the UN:[883]

🟦 Northern Europe ▯ Western Europe 🟥 Eastern Europe 🟩 Southern Europe

[881] NATO (2015) ‘Member States’.

[882] EUROPA (2015) ‘EU countries’.

[883] EUROPA (2015) ‘European region’.



9.2 Appendix 2: Research Keywords

Accountability, anticipation, anticipatory governance, awareness, awareness-raising and education, blocking, censorship, civil liberties, collaboration, computer activism, computer experts, computer technologies, contemporary security, contractual governance, constructivism, cooperation, counter-terrorism, critical information infrastructure, critical infrastructure, cyber-attacks, cyber-incidents, cyber-crime, cyber-criminality, cyber criminals. Cyber-crime Convention, cyber governance, cyber policy, cyber-response, cyber-security, cyber-security education, cyber-security practices, cyber-security rules and regulations, cyber-terrorism, cyber-warfare, decentralised governance, desecuritization, security conventions, ENISA, EP3R, Europe2020, European Communication, European Cyber-crime Centre, European cyber-security directives, European cyber-security recommendations, European cyber-security regulations, European cyber-security strategies, European cyber directive, European security road maps, European security actors, European security action plans, European Union, European Union and critical infrastructure, European Union and cyber-security, Europol, exceptionalism, exceptional measures, filtering, First World War, Foucault, fundamental freedoms, globalisation, global security institutions, governmentality, hackers, hacktivism, hierarchical structures, human security, hybrids, incidents, information computer technologies, infrastructure, (in)securities, internal and external security, international cooperation, international security actors, legislative processes, management of unease, management plans, meta data, meta governance, modernisation, NATO, NATO cyber-security defence, networked security, NIS PPPs, nodal governance, oversight, power, precaution, pre-emption, prevention, private cooperation, private regulation, public-private actors, public-private partnerships, realism, recovery plans, referent objects, regional cooperation, regulatory processes, resistance, resilience and preparedness, risk, risk-governance, risk-management, Second World War, security, security actors, security approach, security decision making, security direction, security governance, security measures, security nodes, security partners, security policies, security professionals, security schools, security-structures, securitization, securitization actors, self-governance, Snowden, social media, spatial spaces, speech-act, state governance, state regulation and practices, surveillance, technical regulation, terrorism, the action plan to implementing the Stockholm Programme, the Cold War, the concept of risk, the Copenhagen School, the Council of Europe, the Council of Europe's Cybercrime Convention, the European Commission, the European Council, the European Court of Justice, The European digital agenda, the European Parliament, The EU, The European Union, the Paris School, the Stockholm Programme, the United Nations, threat, threat policies, transnational cooperation, transparency, vulnerability, vulnerability assessment.

9.3 Appendix 3: Chapter Five[884]

Top Treats	**Current trends**	**Top 10 Emerging Trends**					
		Mobile Computing	**Social Technology**	**Critical Infrastructure**	**Trusted Infrastructure**	**Cloud**	**Big Data**
Drive-by Exploits	Up	Up	Up	Up	-	Up	Up
Worms/ Trojans	Up	Up	Up	Up	-	No change	Up
Code Injection	Up	No change	-	Up	-	Up	-
Exploit Kits	Up	Up	No change	Up	-	-	Up
Botnets	Up	Up	-	No change	-	No change	-
Denial of Service	No change	-	-	No change	Up	No change	-
Phishing	No change	Up	Up	No change	-	-	No change
Compromising Confidential Information	Up	Up	-	Up	No change	Up	Up

[884] Marinos and Sfakianakis (2012),3.

Rogue ware/ Scareware	No change	-	No change	-	-	-	-
Spam	Down	-	No change	-	-	-	No change
Target Attacks	Up	-	Up	Up	No change	Up	No change
Physical Theft/ Loss/Damage	Up	Up	Up	Up	No change	No change	-
Identity Theft	Up	Up	Up	-	No change	Up	Up
Abuse of Information Leakage	Up	No change	Up	-	No change	Up	Up
Search Engine Poisoning	No change	-	-	-	-	-	-
Rough Certificates	Up	-	-	-	Up	-	-

9.4 Appendix 4: Statistic Data Regarding Cyber-crime[885]

Cyber-crime	**Statistic data**	**Demographical information Highest level**	**Demographical information Lowest level**
Identity theft	On average across the EU, 8% of internet users say they have experienced or been a victim to identity theft	Respondents, who are more likely to experience identity theft: • Romania (16%) • Hungary (12%) • UK (12%). • Austria (11%) This includes respondents who have experienced it often: • Romania (5%)	The lowest levels are in: • Slovenia (2%) • Lithuania (2%) • Greece (3%) • Denmark (3%)
Scam email	Around 50% of respondents say that they have received emails fraudulently asking for money and personal details	The highest numbers comes from: • Denmark (54%) • The Netherlands (54%) • Malta (53%) • Sweden (53%) • UK (52%) • Luxembourg	The lowest figures for receiving a scam email can be seen in: • Bulgaria (18%) • Greece (18%) • Poland (19%)

[885] The date from figure one comes from: EC (2012a), 44-57. *Data are collected from all 27 Member States. Participants in the survey are 15+, and the date is collected 10.03.2012, and 25.03.2012. 26.593 interviews are carried out from a population of 408.879.069*. EC (2012a), TS2 (appendix).

		(51%) The proportion that say this has happened to them often is also high in these countries Particularly in: • UK (21%) • Luxembourg (20%)	
Online fraud	An average of 12 % of Internet users in the EU have said that they have experienced online fraud	The proportion who have experienced online fraud is highest in: • Poland (18%) • Hungary (17%) • Malta (16%) • UK (16%)	Respondents, who are less likely to have experienced online fraud are in: • Greece (3%) • Slovenia (6%) • Spain (7%)
Offensive material	Across the EU as a whole, 15% have said that they have accidentally met material, which promotes racial hatred or religious extremism	This number is highest in: • Hungary (30%) • Romania (26%) • Slovakia (26%)	The proportion who have experienced this problem is lowest in: • Denmark (7%) • Greece (9%)
Access to online services/ cyber-terrorism	Averages of 13 % of Internet users have experienced problems in accessing online services because of cyber-attacks.	This number is considerably higher in: • Finland (31%) • The Netherlands (28%)	The proportion who have experienced this problem is lower in: • Greece (4%) • Czech Republic (6%) • Latvia (6%) • Cyprus (7%)

9.5 Appendix 5: Cyber-attacks

	Place	**Attack-type**
1999	Kosovo (the Kosovo crisis). NATO	Blocked access to internet, and repeated disruption of NATO's homepage
2007	Estonia	This three-week long attack blocked websites and froze the entire Internet infrastructure i.e. banks, official documents and email accounts. The cyber-attack came when Estonia was involved in a dispute with Russia over the removal of a Soviet-era war memorial in Tallinn.[886]
2008	Belarus	Radio Free Europe/ Radio Liberty's services

[886] BBC News (2007) 'Estonia hit by 'Moscow cyber war'.

		attacked by DDoS. Few hours' later attacks launched against the Belarus Servers and Seven other RFE/RL webpages in Eastern European and Central Asia/ Middle East region (all within the Russian Federation). The attacks happened on the day for the political opposition protest rally on 26 April in relation to the 22nd anniversary of the Chernobyl nuclear disaster. This attack is considered to be launched in order to limit the freedom of expression by Belarus.[887]
	Lithuania	Attack on the private and public sectors with more than 300 attacks (95 % of the private sector, and 5 % against governmental webpages. The attacks are seen as a reaction to the adoption of a law prohibiting Nazi and Soviet symbols. There were strong reactions to this legislation from the Russian minority in Lithuania, Russia and Belarus, which included the cyber-attack.[888]
	Georgia	Attacks on the government's websites and servers as a part of state-terrorism. The attacks happened during the Georgia/Russia conflict. These cyber-attacks did not do any physical harm, but they weakened the Georgian government during the conflict as it has a major impact on communication.[889]
	Project Chanology	The group Anonymous attacked the Church of Scientology with a DDOS attack- over a couple of days- hitting the webpages with a serial attack. This was a reaction to an interview of actor Tom Cruise on the internet, where he praised the Church.[890] The attacks were the beginning of a long-term campaign against the church.
2009	The United States	Cyber-attack on a US electrical grid. The attackers left behind software that could disrupt the system. Allegedly, this attack came from cyber-spies from Russia and China.[891]
	South Korea and the U.S.	Widespread cyber-attacks towards several U.S. government agencies and South Korean government web-pages. These attacks slowed down, and in some cases, shut down websites. The attack is believed to come from North Korean sympathisers.[892]
2010	Google/ China	Google-attack, assumable by/ or supported by Chinese authorities as an escalation of a long history of run-ins between these two parties

[887] Tikk et al (2010),47.
[888] Tikk et al (2010),63.
[889] NATO (2011b) 'New threats: the cyber dimension'. Tikk et al (2010),89.
[890] McMillan (2008) 'Hackers hit Scientology with online attack'.
[891] EURACTIV (2011) 'Cyber-attacks now the most feared EU energy threat'.
[892] BBC News (2009) 'Governments hit by cyber attack'.

		(China and the U.S./Google): the dispute concerned Google’s unfiltered research engine and Chinese censorship. The attack targeted the email accounts of Chinese human rights activists and computers linked to the infrastructure of Google and other U.S. firms.[893]
	Iran	A severe attack on Iranian power plants by a ‘Stuxnet’ worm. This Trojan virus has infected approximately 45,000 industrial Siemens control systems worldwide. The virus manipulated technical processes related to nuclear power plants in Iran.[894]
	Operation Pay-Back	Operation Pay-back launched by the hacking group Anonymous. This wave of attacks was Introduced to target the music industry and an opponent to internet piracy.[895] The core element in their activities is to uncover corruption and fight oppression.[896] Later, expansion of this operation included new objectives.[897]
	Myanmar	DDoS attack launched 20 days before the first election in the country for 20 years. Allegedly, the government was behind this massive attack. This sophisticated attack involved several types of DDoS types from a variety of sources.[898]
	The United States	This is a part of the Pay-back operation. This operation targeted firms that have withdrawn services from Wikileaks i.e. VISA, PayPal, and MasterCard (Amazon was considered, but not attacked).[899] This was a DDoS attack, using Anonymous attack-tool ‘LOIC’. When a person installed the tool on their pc, it enrolled the device into a voluntary botnets, which then bombarded the target site with data until it broke down.[900]
2011	Japan	Japan’s weapon makers were attacked, i.e. Data on missiles, submarines and nuclear power plants. Viruses were in more than 80 servers and computers.[901]
	The United States	Chinese-based hackers gained full functional control of computers at NASA.[902] Allegedly, the attackers obtained “full system access” and would have been able to “modify, copy, or delete sensitive files” or “upload hacking

[893] BBC News (2010c) ‘Google in ’new approach’ in China’.
[894] NATO (2011b).
[895] Laville (2012).
[896] Mansfield-Devine (2011) 5.
[897] Laville (2012).
[898] BBC News (2010b) ‘Burma hit by massive attack ahead of election’.
[899] BBC News (2010a).
[900] BBC News (2010d) ‘Pro-Wikileaks activists abandon amazon cyber attack’.
[901] BBC News (2011a) ‘Japan defence firm Mitsubishi heavy in cyber attacks’.
[902] BBC News (2013j) ‘Wall Street journal 'also victim of China hacking attack'.

		tools to steal user credentials and compromise other NASA systems”.[903]
	South-Korea	Leading governmental web pages have been attacked by DDoS attacks believing that the hackers injected malware into a couple of peer-to-peer file-sharing websites. Among those attacked were government ministers, the National Assembly, the Military HQ, the U.S. Forces, and major banks.[904]
2012	Israel	Group Anonymous launched a new campaign: OpIsrael. A Series of cyber-attacks launched against websites in Israel. DDoS attack. This followed a threat by the Israeli government to cut all Gaza’s telecommunication links. The hackers posed a website stating, “We are Anonymous and NO ONE shuts down the internet on our watch”.[905]
	China	The group Anonymous claims to have defaced almost 500 websites in China. The group attacked in the mass defacement government sites, official agencies, trade groups and many others. A message put on the hacked sites said the attack was a protest against the Chinese government's strict control of its citizens.[906]
	Interpol	Interpol's website appears to have been attacked after the international police agency had arrested 25-suspected members of the hacking activist group Anonymous in Europe and South America. The website went down briefly as supporters of Anonymous made online claims that it had been targeted following the arrests in Argentina, Chile, Colombia and Spain. [907]
	The Vatican	The group Anonymous took down the Vatican's website in retaliation for the "corruption" of the Roman Catholic Church. The action came just after the FBI issued charges against an individual alleged to be a member of Anonymous, and four people alleged to be principal members of LulzSec.[908]
	The United Kingdom	The hacking group Anonymous warned it would launch online attacks every weekend, following claims it disrupted access to the Home Office website. The Home Office web

[903] BBC News (2012c) ‘Hackers had 'full functional control' of Nasa computers’.
[904] BBC News (2011d) ‘South Korea hit by cyber attacks’.
[905] BBC News (2012a) ‘Anonymous hacker group attacks Israeli websites’.
[906] BBC News (2012b) ‘Chinese websites 'defaced in Anonymous attack'.
[907] Quinn (2012) ‘Interpol website suffers 'Anonymous cyber-attack'.
[908] Batty (2012) ‘Vatican becomes latest Anonymous hacking victim’,

		page broke down for a couple of hours after a DDoS Attack.[909]
	Israel	Israeli national airline, El Al and the Tel Aviv Stock Exchange. This was a DDoS attack, which disrupted the webpage. It is believed that a Saudi computer hacker activated this campaign.[910]
	WikiLeaks	Disruption of the Wikileaks website by DDoS attacks for more than a week. The website was flooded with 10 gigabits per second, which made it slow and unresponsive.[911]
	India	Members of the internet hacking group Anonymous staged protests across 16 cities in India, against what they say is internet censorship in the country. The group Anonymous carried out a number of "Denial of Service" (DDOS) attacks, against more than 15 sites, including the Indian Supreme Court, two political parties and the Indian telecoms providers.[912]
	Saudi Arabian Oil Company (Aramco) and RasGas of Qatar	A Sophisticated virus, 'Shamoon', infected computers. This virus included a routine (a Wiper) coded to self-execute. This replaced essential system files with an image of a burning U.S. flag, and it put in a 'garbage date' overwriting all the real data on the infected computers. Result, over 30,000 computers replaced.[913]
	Capital One Financial Group and BB&T Corp	Attack on U.S. Banks; Capital One Financial Group and BB&T Corp. DoS prevented customers from accessing their internet-banking information. This attack is linked to the attack mentioned above. The group 'Qassam Cyber Fighters' claimed responsibility. The Iranian government allegedly supported these attacks.[914]
	HSBC	The UK bank was subjected to a large-scale attack, which disrupted online services, as the attack targeted internet banking. DDoS attack. No indication of who was behind the attack.[915]
	Germany	A power utility specialising in renewable energy was hit by a serious cyber-attack, which lasted for 5 days and brought down the internet communication systems. This is the

[909] BBC News (2012e) 'The hacking group Anonymous says it will launch online attacks every weekend, following claims it disrupted access to the Home Office website'.

[910] Knell (2012) 'New Cyber Attacks hits Israeli Stock Exchange and Airline'.

[911] BBC News (2012f) 'Wikileaks websites back Online after DDoS Cyber attacks'.

[912] Vaidyanathan (2012) 'Hacking group Anonymous takes on India internet 'censorship''.

[913] Mount. (2012) 'New Cyber attacks on U.S. Banks; Iran suspected'.

[914] Mount (2012).

[915] Sky News (2012) 'HSBC Suffers 'large scale' cyber attack'.

		first confined digital assault against European grid operators.[916]
2013	Australia	Australia's central bank confirmed that hackers had targeted it. The attack contained a malware application, which had managed to bypass existing security controls, but was not able to spread through the computer system. China is considered involved in the attack.[917]
	South Korea	Virus attack disrupted and paralysed the computer networks of broadcasters and banks in South Korea (i.e. two South Korean banks, Shinhan Bank and Nonghyup, and three TV stations KBS, MBS and YTN.) There were also reports of skulls popping up on some computer screens. This indicates that the hackers had installed malicious code in the networks.[918] Allegedly it was an act by North Korea
	The United Kingdom, France and The United States	Syrian Hackers targeted a series of western media organisations in an attempt to cause disruption and spread support for the Syrian regime. The Syrian Electronic Armey (SEA) claimed responsibility. There had previously been random attacks, i.e. the broadcaster of Al-Jazeera, the Government of Qatar, where attacks were based on ‘phishing’.[919]
	The United Kingdom	Hundreds of thousands of Britons were unsuspecting participants in one of the internet's biggest cyber-attacks ever – because their broadband router had been subverted. Spamhaus, which operates a filtering service, which was used to weed out spam emails, went under attack since 18 March after adding a Dutch hosting organisation called Cyberbunker to its list of internet sites. [920]
	The United Kingdom	The web-page of Kent police, and Oxford and Cambridge Universities were attacked by a DDoS attack overwhelming them with attacks requesting information. This brought down the web pages for more than 3 hours.[921] Two UK citizens were behind the attacks.
	South-Korea	The website of the presidential office was one of several official and media sites hit by an apparently co-ordinated attack. The incident came on the anniversary of the start of the 1950-53 Korean War. Messages on the hacked webpages claimed that the hacking collective Anonymous was responsible.

[916] EURACTIV (2012).

[917] BBC News (2013c) ‘Australia's central bank targeted by Hackers’.

[918] BBC News (2013i) ‘South Korea network attack' a computer virus''.

[919] Hopkins and Harding (2013) ‘Pro-Assard Syrian hackers launching cyber-attacks on Western media’

[920] Arthur (2013) ‘Internet slows down after DNS attack on Spamhaus’.

[921] BBC News (2013h) ‘Kent man admits Oxbridge and police force cyber attacks.

		However, they have denied. It is more likely it is North Korea.[922]
	Australia	Hackers attacked the websites of the Australian police and Reserve Bank. This was part of an ongoing row over reports, which stated that Canberra spied on Jakarta officials. The row caused diplomatic tensions and sparked protests in Indonesia. This was a DDoS attack, and it was presumed to be carried out by hackers form Indonesia[923].
	The United Kingdom	The RBS Group, which includes RBS, NatWest and Ulster Bank, was attacked. However, NatWest was worst affected by the "deliberate" disruption.[924] NatWest was the victim of a "deliberate attempt to disrupt" its operations by using a distributed denial of service attack (DDoS).[925]
2014	The United States	The news aggregator Feedly and the data storage company Evernote were attacked. Hackers used DDoS to prevent users from accessing the service. Caused by an unknown perpetrator.[926]
	Europe and The United States	A massive DDoS attack hit EU- and US-based servers. Security companies reported it to be even more powerful than last year's Spamhaus attacks.[927]
	Cyber-space	A DDoS attack on virtual currency Bitcoin briefly took down its ability to process payments for a while.[928]
	The United States	Internet registration firm, Namecheap, was temporarily overwhelmed by a simultaneous DDoS attack on 300 of the websites it registers.[929]
	The United States	bit.ly, which creates shortened addresses for websites like Twitter, said it was also knocked out briefly in February by a DDoS attack.[930]
	NATO	Unidentified hackers attacked several public NATO websites with DDoS cyber-attacks in what appeared the latest escalation in cyberspace over growing tensions over Crimea. A group calling itself "cyber berkut" claimed to be behind the attack as a response over what they saw as NATO interference in their country.[931]

[922] BBC News (2013e) 'Cyber attack hits South Korea websites'.

[923] BBC News (2013d) 'Australia sites hacked amid spying row with Indonesia'.

[924] BBC News (2013f) 'NatWest online services hit by cyber attack'.

[925] BBC News (2013g) 'NatWest cyber attack disrupted Ulster Bank website'.

[926] Shah (2014) 'Evernote latest to be struck by DDoS attack'. Kelion (2014) 'Feedly and Evernote struck by denial of service cyber-attacks'.

[927] RT (2014) ''Biggest ever'? Massive DDoS-attack hits EU, US'.

[928] Apps (2014) 'DDoS cyber attacks get bigger, smarter, more damaging'.

[929] Apps (2014).

[930] Apps (2014).

[931] The Telegraph (2014) 'Nato websites targeted in cyber attack over Crimea stance'.

	Norway	A cyber-attacks against the central bank Norges Bank [The Bank of Norway] and eight major banks, financial institutions and telecommunications were among the most serious ever to hit the country's online networks. Group Anonymous took responsibility for the DDoS attacks.[932]
	The United States	"Lizard Squad" took down several popular online video game networks and possibly diverted an American Airlines jet carrying a Sony executive.[933] The hacker group launched a DDoS attack towards four game operators, i.e. Battle.net, EVE online, League of Legends and large parts of Sony/ PlayStation. The Chief Executive for Sony Online Entertainment, John Smedley, announced on Twitter that he would fly from Dallas to San Diego over the weekend. The hackers saw this and made a veiled threat about bombs on his plane.[934]
	Japan/ The United States	Computer hackers forced Sony Pictures Entertainment to shut down its systems. A skull appeared on computer screens along with a message threatening to release data "secrets" if the demands were not met. The message showed "#GOP" indicating a group called Guardians of Peace was behind the attack.[935] North Korea refused to deny involvement in a cyber-attack on Sony Pictures that came ahead of the release of a film about an assignation of the country's leader Kim Jong-un.[936]
	South-Korea	KHNP, part of state-run utility Korea Electric Power, said that its computer systems had been hacked but only non-critical data had been stolen, and reactor operations were not at risk. A hacker demanded the shutdown of three reactors and in Twitter messages threatened "destruction" if the demand was not met. South Korea's nuclear power operator said that cyber-attacks on non-critical operations at its headquarters continued but the country's nuclear power

[932] News in English. No (2014) 'Extent of cyber attacks revealed'.

[933] NewsMax (2014) 'Hackers took down Sony's PlayStation network To show Lax security'.

[934] Pagliery (2014) 'Hackers attack Sony PlayStation network'. Frank (2014) 'Hackere lagde flere netværk ned og fik ændret flyrute'.

[935] BBC News (2014d) 'Sony Pictures computer system hacked in online attack'.

[936] BBC News (2014a) 'North Korea refuses to deny Sony Pictures cyber-attack'. McCurry (2014a) 'South Korean nuclear operator hacked amid cyber-attack fears'.

		plants was operating safely and was secure from attacks.[937]

9.6 Appendix 6: Infrastructure[938]

Sectors	Industries
Energy	• Electricity • Natural gas • Oil
Information and Communication Technology (ICTs)	• Telecommunication (including satellites) • Broadcasting systems • Software, hardware and networks (Including the Internet)
Traffic and Transportation	• Shipping • Aviation • Rail transport • Road traffic • Logistic
Healthcare	• Healthcare • Medicine and vaccinations • Laboratories
Water supply	• Dams • Storage • Treatment and distribution networks
Finance and Insurance	• Banks • Stock exchange • Insurance companies • Financial services
Government and Administration	• Government • Parliament • Legal institutions • Emergency services
Nutrition and Agriculture	• Food trade • Agriculture
Media and Cultural Assets	• Radio • Press • Symbolic buildings

9.7 Appendix 7: EU Security Agencies

Security Agency	Role
European Network and Information Security Agency (ENISA)	• This agency has a linking role in the European framework • It aims to develop expertise to enhance cooperation

[937] The Guardian (2014a) 'Cyber-attacks on South Korean nuclear power operator continue'.

[938] OSCE (2013) 'Good practices guide on non-nuclear critical energy infrastructure protection (NNCEIP) from terrorist attacks focusing on threats emanating from cyberspace'.

	between the public and private sectors and to provide assistance to both the Commission and the Member States • It is crucial to cyber-terrorism, as the EP3R is positioned directly in this agency[939]
The EU (2012)	• This agency aims to support the European institutions to protect themselves against intentional and malicious cyber-attacks • This initiative has launched its own CERT: CERT-EU directed towards EU institutions, agencies, and bodies [940]
The European Public-private Partnership for Resilience (EP3R)	• This agency aims to help businesses/ public authorities to share experience and information • To ensure adequate and consistent level of prevention, detection, emergency and recovery measures • Is complementary to the European Forum for Member States (EFMS)[941]
The European Forum of Member States (EFMS)	• This forum has developed European principles and guidelines for the resilience and stability of the Internet • It aims to develop and share information and good policy practices, and to develop National/Governmental CERTs[942]
The European Information Sharing and Alert System (EISAS)	• This agency has planned to promote and develop CERTs teams • Focused on citizens and small-medium businesses[943]
European Cybercrime Centre (EC3)	• This agency is a part of Europol's governance structure • It is directed to operational cooperation, to exchange knowledge, to pool European expertise and to support Member States and their cyber-crime investigations • Creates a link between law-enforcement and the judiciary[944]
The Network and Information Security Public-Private Platform (NIS)	• This agency is not established yet. However, it was launched June 2013 and includes relevant public and private stakeholders • Aims to work across the value chain to identify good practices and create favourable market conditions for developing and adopting security ICT solutions[945]

9.8 Appendix 8: Regulatory Framework

[939] EC (2010i), 5.
[940] CERT-EU (2013) 'About Us'.
[941] EC (2010h), 5.
[942] EC (2010i), 5.
[943] EC (2009b), 2.
[944] EC (2013c). EC (2012b), 4.
[945] EC (2013e).

Regulation	Classification	Content
Council of the European Union (2003) **Council Resolution on a European approach towards a culture of network and information security**[946]	Council Resolution Cyber-security	RECALLING: • the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Network and Information Security: Proposal for a European Policy Approach; • the Council Resolution of 30 May 2001 on the "eEurope Action Plan: Information and Network Security"; • the Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security; • the eEurope 2005 action plan endorsed by the Seville European Council in June 2002; • the Opinion of the European Parliament on the European Commission Communication on • Network and Information Security: Proposal for a European Policy Approach • Opens up for dialogue about enhancing security, i.e. development of information society services, network and information security to improve the daily life of citizens, businesses and public administrations and contributing to the proper functioning of the Internal Market • Further develop a comprehensive European strategy for network and information security and strive towards "a culture of security" taking into account the importance of international cooperation • Progress a valuable model for developing security policies • Respect privacy rights. Build up confidence in data protection, i.e. handled accurately, confidentially and reliably • Developing a culture of security • Develop and deployment an appropriate skill base in the field of network and information security • Develop a coherent security policy t at European level including cross-pillar transparency and cooperation • Fulfil the commitments made in the Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security has to be continued[947]
European Commission (2004) **Communication on a European Programme for**	Communication Terrorism	• Forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving Critical Infrastructures (CI) • Build on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks"

Critical Infrastructure Protection in the Fight against Terrorism[948]		• Propose a European Programme for Critical Infrastructure Protection (EPCIP) set up by the Commission of a Critical Infrastructure Warning Information Network (CIWIN).[949]
CoE (2004) Convention on Cyber-crime[950]	Convention Cyber-crime	• Develop a common criminal policy to protect society against cyber-crime. • Decrease the risks of computer networks and electronic information, enhance cooperation between states and the private industry, • Enhance the efficiency of operations based on increased, rapid and well-functioning international cooperation, prevent and protect ICTs against misuse, • Criminalise particular conduct, adopt powers sufficient for combating cyber-crime by facilitating their detection, investigation, and prosecution on national and international levels, • Ensure a proper balance between the interests of law enforcement, and respect for fundamental human rights.[951] • The main areas of the Convention are offences against the confidentiality, integrity and availability of computer data and systems, i.e. illegal access and interception, data and system interference.[952] •
European Council (2005) **Council Framework Decision 2005/222/JHA on attacks against information systems**[953]	Framework Decision Cyber-security	• The Objective is to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States • The objective of this Framework Decision is to improve cooperation between judicial and Member States in the area of attacks against information systems[954] • Approximating criminal law in Member States. • Introduced EU legislation to deal with offences such as illegal access to information systems, illegal system interference and illegal data interference, as well as specific rules on the liability of legal persons, jurisdiction and exchange of information[955]
European Commission (2006)	Communication Terrorism	• A key element of EPCIP is the Directive on the identification and designation of European Critical Infrastructures, which identifies the ICT sector as a future priority sector

[948] EC (2004) 'Communication on a European programme for critical infrastructure protection in the fight against terrorism' COM(2004) 702 final. EC (2006a) 'A European programme for critical infrastructure protection'.
[949] EC (2004). EC (2006a).
[950] CoE (2001).
[951] CoE (2001).
[952] CoE (2001).
[953] Eco (2005) Council Decision Framework on attacks against information systems.
[954] Eco (2004).
[955] EC (2010a).

Communication on a European Programme for Critical Infrastructure Protection[956]		• Another important element of EPCIP is the Critical Infrastructure Warning Information Network (CIWIN)[957] • The communication sets out the principles, processes and instruments proposed to implement EPCIP • The aims to respond are not confined to terrorism, but also include criminal activities, natural hazards and other causes of accidents, using an all-hazards approach • The general objective of EPCIP is to improve the protection of critical infrastructure in the European Union (EU). • The legislative framework for the EPCIP consists of the following: o A procedure for identifying and designating European critical infrastructure and a common approach to assessing the need to improve the protection of such infrastructure o measures designed to facilitate the implementation of EPCIP, including an EPCIP action plan, the Critical Infrastructure Warning Information Network (CIWIN), the setting up of Critical Infrastructure Protection (CIP) expert groups at EU level, CIP information sharing processes, and the identification and analysis of interdependencies o Support for EU countries regarding National Critical Infrastructures (NCIs) that may optionally be used by a particular EU country, and contingency planning o An external dimension o Accompanying financial measures, and in particular the Specific EU Programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-13, which will provide funding opportunities for CIP related measures[958]
European Commission (2006) **Communication for a Strategy for a secure Information society**[959]	Communication Cyber-security	• Sets out the revitalised strategy and provides the framework to carry forward and refine a coherent approach to Network and Information security, and on Fighting spam, spyware and malicious software • This strategy strengthens the role, on tactical and operational levels, of the European Network and Information Security Agency (ENISA), established in 2004 to contribute to the goals of ensuring a high and effective level of NIS within the Community and developing a culture of NIS for the benefit of EU

[956] EC (2006a).

[957] EC (2006a).

[958] EC (2006b) 'Communication on a European programme for critical infrastructure protection'.

[959] EC (2006b). EC (2007b) 'Towards a general policy on the fight against cyber crime'.

		citizens, consumers, enterprises and administrations[960] • Further develop a dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnership and empowerment • Developed a three-pronged approach to tackling the development: ○ Specific network and information security measures ○ The regulatory framework for electronic communications (which includes privacy and data protection issues) ○ The fight against cyber-crime. • This Communication sets out the strategy and provides the framework to carry forward and refine a coherent approach to NIS.[961] •
European Commission (2007) **Communication towards a general policy on the fight against cyber-crime**[962]	Communication Cyber-security	• The objective is to strengthen the fight against cyber-crime at national, European and international level • Further development of a specific EU cyber-crime policy. The focus are on the law enforcement and criminal law dimensions and the policy will complement other EU actions to improve security in cyber-space in general • The policy will include: ○ Improved operational law enforcement cooperation ○ Better political cooperation and coordination between Member States ○ Political and legal cooperation with third countries ○ Awareness raising ○ Training ○ Research • A reinforced dialogue with industry and possible legislative action[963]
European Commission (2008) **Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to**	Directive Cyber-security	• The 'European Programme for Critical Infrastructure Protection (EPCIP)' sets out the overall 'umbrella' approach to the protection of critical infrastructures in the EU. • The objectives of EPCIP are fully consistent with this proposal and the Directive should apply without prejudice to Directive 2008/114. • EPCIP does not oblige operators to report significant breaches of security and does not set up mechanisms for the Member States to cooperate and respond to incidents[965]

[960] EC (2006b). EC (2009b).
[961] EC (2006b).
[962] EC (2007b).
[963] EC (2007b).
[965]EC (2013i). EC (2013b).

improve their protection[964]		
European Commission (2009) **Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large-scale cyber-attacks and cyber disruptions: enhancing preparedness, security and resilience'[966]**	Communication Cyber-security	• A 'CIIP action plan' to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures. • Stimulate and support the development of a high level of preparedness, security and resilience capabilities both at national and European level.[967] • The CIIP action plan is built on five pillars: ○ Preparedness and prevention, ○ Detection and response, ○ Mitigation and recovery, ○ International cooperation ○ Criteria for European Critical Infrastructures in the field of ICT. • It sets out the work to be done under each pillar by the Commission, the Member States and/or industry – supported by the European Network and Information Security Agency (ENISA).[968]
European Council (2009) The Stockholm programme[969]	Security programme From 2010 – 2015 Security	• The Stockholm Programme sets out the European Union's (EU) priorities for the Area of Justice, Freedom and Security for the period 2010-14. • Building on the Tampere and Hague programmes. • Provide a secure Europe where the fundamental rights and freedoms of citizens are respected, the Stockholm Programme focuses on the following priorities: ○ Europe of Justice, Europe that protects, Access to Europe, Europe of Solidarity, Europe in a globalised world. ○ Under the heading' Europe that protects', it is focusing on the following categories: trafficking in human beings; sexual abuse, sexual exploitation of children and child pornography; cyber-crime; economic crime, corruption, counterfeiting and piracy, drugs.[970]
European Commission (2009) **Communication on protecting Europe from large-scale**	Communication Cyber-security	• Focuses on prevention, preparedness and awareness • Defines a plan of immediate actions to strengthen the security and resilience of CIIs • Addresses the challenges and priorities for network and information security (NIS) policy. • The proposed actions are also complementary to those to prevent, fight and prosecute criminal and terrorist activities targeting CIIs

[964] EC (2013i).
[966] EC (2009b). EC (2011a).
[967] EC (2009b). EC (2011a).
[968] EC (2009b) EC (2011a).
[969] EU (2010j).
[970] EU (2010j).

cyber-attacks and disruptions: enhancing preparedness, security and resilience[971]		- In line with current and prospective EU research efforts in the field of network and information security, as well as with international initiatives in this area.[972]
European Commission (2010) **Delivering an area of freedom, security and justice for Europe's citizens. Action Plan Implementing the Stockholm Programme.**[973]	Action Plan Security	- Supporting regulation - The aim is to deliver those priorities outlined in the Stockholm Programme; both at European and global level, - Ensuring that citizens benefit from progress made in the area of freedom, security and justice. - Develop European response to European and global challenges.[974]
European Commission (2010) **The EU Internal Security Strategy in Action: Five steps towards a more secure Europe**[975]	Strategy (internal) Security	- Forwards a shared agenda for Member States, the European Parliament, the Commission, the Council, agencies and others, including civil society and local authorities. - Cooperation with the European security industry in which manufacturers and service providers work closely together with end-users. - The aim is to deliver responses to the security challenges, i.e. strengthening and developing the European model of a social market economy put forward in the Europe 2020 strategy.[976] - A coordinated approach to police cooperation, border management, criminal justice cooperation and civil protection. - Address all the common security threats from terrorism and organised crime, to safety concerns related to manufactured and natural disasters. - A complementary policy ensuring the preparedness and resilience of Europe's networks and ICT infrastructure.[977]
European Commission (2010) **The Digital Agenda for**	Communication Cyber-crime	- Build on a shared understanding that trust and security are fundamental preconditions for the wide uptake of ICT and therefore for achieving the objectives of the ‘smart growth’ dimension of the Europe 2020. - Set out to define the key enabling role that the use of

[971] EC (2009b).
[972] EC (2009b).
[973] EC (2010e).
[974] EC (2010e).
[975] EC (2010i).
[976] EC (2010i).
[977] EC (2010i). EC (2010e).

Europe[978]		Information and Communication Technologies (ICT) will have to play if Europe wants to succeed in its ambitions for 2020 (Europe 2020). • Maximise the social and economic potential of ICT, i.e. the internet, a vital medium of economic and societal activity: for doing business, working, playing, communicating and expressing ourselves freely. • Accelerate innovation, economic growth and improvements in daily life for both citizens and businesses to deploy a more effective use of digital technologies. • The strategy emphasises the need for all stakeholders to join their forces in a holistic effort to ensure the security and resilience of ICT infrastructures. • Focusing on: ○ Prevention, preparedness and awareness • Develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyber-attacks and cyber-crime[979]
European Commission (2010) **Europe 2020 Strategy**[980]	Strategy Security	• Strategy to exit the crisis and prepare the EU economy for the challenges of the next decade. • Sets out a vision to achieve: ○ High levels of employment, a low carbon economy, productivity, and social cohesion, ○ To be implemented through concrete actions at EU and national levels. • The battle for growth and jobs requires involvement at top political level and mobilisation from all actors across Europe.[981] • Europe has identified new engines to boost growth and jobs. These areas are addressed by 7 flagship initiatives. ○ One of these is the digital agenda for Europe.[982]
European Commission (2011) **Communication on Critical Infrastructure Protection 'Achievements and next steps: towards global cyber-security'**[983]	Communication Cyber-security	• Follows the results achieved since the adoption of the CIIP action plan in 2009. • It describes the next steps planned for each action at both European and international level. • Focuses on the global dimension of the challenges and the importance of improving cooperation among Member States and the private sector at national, European and international level.[984] • Promotes a global culture of risk management including coordinated actions to prevent, detect, mitigate and react to all kinds of disruptions, whether man-made or natural, as well as to prosecute related cyber-crimes.

[978] EC (2010b).
[979] EC (2010b) EC (2009b).
[980] EC (2010b).
[981] EC (2010b).
[982] EC (2014b) 'Flagship initiatives'.
[983] EC (2011a).
[984] EC (2011a).

		• This includes: ○ Promote principles for the resilience and stability of the Internet ○ Build strategic international partnerships ○ Develop trust in the cloud ○ Enhance EU preparedness by establishing a network of well-functioning National/Governmental CERTs by 2012 ○ A European cyber-incident contingency plan by 2012 and regular pan European ○ Cyber exercises ○ European coordinated efforts in international fora and discussions on enhancing security and resilience of Internet[985]
European Commission (2010) **A proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA[986] /** **European Commission (2013)** **The Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA[987]**	Proposal for a Directive/ Directive Cyber-security	• Aims to strengthen the fight against cyber-crime by approximating Member States' criminal law systems • Improving cooperation between judicial and other competent authorities. • Introduces provisions to deal with new forms of cyber-attacks, in particular botnets • A proposal for a new mandate to strengthen and modernise the European Network and Information Security Agency (ENISA) in order to boost trust and network security ○ Strengthening and modernising ENISA will help the EU, Member States and private stakeholders develop their capabilities and preparedness to prevent, detect and respond to cyber-security challenges[988] • Extend the scope by including a set of new offences, and new penalties for the Member States to impose. • Aims to facilitate the prevention of cyber-crime by improving cooperation, which is important to manage the growing number of cyber-risks.[989] • The preamble of the legislation mentions the use of botnets and malicious software specifically, as well as illegally obtained passwords, which for long has been a particular concern.[990] • These measures will not only tackle attacks against information systems, but also financial cyber-crime, illegal Internet content, the collection, storage, transfer of electronic evidence, and more detailed jurisdiction rules. • This proposal is developed as an alternative to the CoE's Convention on Cyber-crime and is thought to work as a parallel to it.[991]
European Commission and	Communication	• The objective of the strategy is to ensure a secure and trustworthy digital environment, while promoting and

[985] EC (2011a).
[986] EC (2010k).
[987] EU (2013).
[988] EC (2010k). EC (2011a),3.
[989] EU (2013).
[990] EU (2013).
[991] EC (2010a),6.

High Representative of the European Union for Foreign Affairs and Security Policy (2013) **Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace**[992]	Cyber-crime	protecting fundamental rights and other EU core values • The proposal is the main action of the Strategy • Further actions under the Strategy in this area focus on raising awareness, developing an internal market for cybersecurity products and services, and fostering R&D investment • These actions will be complemented by others aimed at stepping up the fight against cyber-crime and building an international cybersecurity policy for the EU[993]
European Commission (2013) **Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union**[994]	Proposal Cyber-crime	• The aim is to ensure a high common level of network and information security (NIS) • Improving the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies • Requires the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures, such as: ○ Energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc.) ○ as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities[995]

[992] EC/HREUFASP (2013).
[993] EC (2013i).
[994] EC (2013i).
[995] EC (2013i).