Cyber Security in the European Union:

An Historical Institutionalist Analysis of a 21st Century Security Concern

Robert Scott Dewar

MA (Hons.), MSc

Submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy

University of Glasgow

School of Social and Political Sciences

College of Social Sciences

December 2016

Abstract

This thesis uses cyber security, an important topic in today's world, as a vector for analysis in order to contribute to a better understanding of the European Union (EU)'s policy-making processes. Although EU policy has received extensive scholarly attention, cyber security policy is under-researched, a gap in current literature this thesis addresses. The goal of the thesis is to understand why the Union adopted and maintained a socio-economic approach to cyber security when other actors added military and defence considerations. The thesis employs an historical institutionalist (HI) framework to examine the long-term institutional and ideational influences underpinning policy development in this area between 1985 and 2013. This was achieved using a longitudinal narrative inquiry employing an original, conceptual content analysis technique developed to gather data from both relevant EU *acquis communautaire* and over 30 interviews.

There were three main findings resulting from this analysis, two empirical and one theoretical. The first empirical finding was that the EU's competences established an institutional framework – a set of rules and procedures – for policy development in this sector. By restricting the EU's capacity to engage in military or national security-oriented issues, its competences required it to respond to emerging security matters from a socio-economic perspective. The second empirical finding was that there exists a specific discourse underpinning EU cyber security policy. That discourse is predicated upon a set of five ideational elements which influenced policy continuously between 1985 and 2013. These five elements are: maximising the economic benefits of cyberspace; protecting fundamental rights; tackling cyber-crime; promoting trust in digital systems and achieving these goals through facilitating actor co-operation. Throughout the thesis the argument is made that the EU adopted and maintained its socio-economic policy as a result of an interaction between this ideational discourse and the institutional framework provided by competences. This interaction created a linear, but not deterministic path of policy development from which the EU did not deviate. The third, theoretical, finding relates to the HI mechanisms of path dependency and punctuated equilibrium. The EU's policy discourse was exposed to major stresses after 2007 which, according to punctuated equilibrium, should have caused policy change. Instead, those stresses entrenched the Union's discourse. This demonstrates an explanatory flexibility not normally associated with punctuated equilibrium. The findings of the thesis have implications for policy practitioners by providing a way to identify underlying ideational dynamics in policy development. Due to a combination of empirical and conceptual findings, the thesis provides a potential basis for future research in EU policy development and HI analyses.

Contents

List of Tables

List of Diagrams

Acknowledgments

As anyone who has ever undertaken a PhD knows, there is a huge phalanx of people who deserve thanks and acknowledgement when the thing is finally completed. I am grateful to all those with whom I have discussed the thesis, its content and concepts and who have provided invaluable insights. I am indebted and grateful to my supervisors, Drs Eamonn Butler and Brandon Valeriano, who supported me and guided me through not only this project but all the logistical challenges that came with it.

I must also thank the various members of the Politics Department at the University of Glasgow who have helped out over the last four years with advice, ideas and sources of invaluable information, and especially Maggie Nicol and Eileen Douglas who frequently provided sympathetic ears and welcome laughs. I must also thank Bethia Pearson for her counsel and for keeping me grounded, and Haley Cross for putting up with me as an office-mate.

I am very grateful to all those professionals and practitioners who agreed to meet with me during the fieldwork phase of the thesis and who shared their time, ideas and experiences as interviewees for this research. I am also grateful to the University of Glasgow's Centre for, Russian, Central and East European Studies (CRCEES) and the Universities' Association for Contemporary European Studies (UACES) for fieldwork travel awards. Particular thanks have to go to Terry Dorrity and Lydia Laura who very kindly let me stay in their home in Brussels twice during fieldwork, and who secured a number of high-level interviews on my behalf.

I would also like to thank my new colleagues at ETH Zürich – Prof. Andreas Wenger, Dr Myriam Dunn Cavelty, Dr Tim Prior, Richard Fueglister and Marie Baezner – who gave me a fantastic career opportunity but still allowed me the time and space to complete the thesis. I must particularly thank Myriam, Dr Matteo Bonfanti and Dr Matthias Leese who helped immensely by reading drafts of the thesis and sharing their thoughts.

Finally, many, many thanks have to go to my family. Huge thanks to my parents Betty and Peter, who helped and supported me in so many ways throughout this endeavour, in particular helping with funding, proofreading so many successive drafts and occasional washing and ironing. Thanks also to my parents-in-law Hamish and Anne, who so very kindly let me turn their home into a writing retreat for several weeks and to my Aunt Isabel

and Uncle Sandy who helped kick-start the whole process by supporting me through my MSc.

My most heartfelt thanks have to go to my wife Shona, who not only gave me 100% support over the last four years, but sacrificed a great deal of time and effort, gave me some great insights, helped produced the diagrams used in this thesis and never stopped believing that I could accomplish this feat. She put up with the ups and downs and kept the coffee flowing, never stopping believing for a moment. Thank you also to our beautiful daughter, Ädeline, who joined us for the final furlong and whose smiles, giggles and gurgles always cheered and inspired. Thank you to you both.

Author's declaration

I declare that except where explicit reference is made to the contribution of others, that this dissertation is the result of my own work and has not been submitted for any other degree at the University of Glasgow or any other institution.

Signature: 

Printed Name: ROBERT SCOTT DEWAR

Abbreviations

AEI	University of Pittsburgh's Archive of European Integration
BEPA	Bureau of European Policy Analysis*
CAQDAS	Computer assisted qualitative data analysis software
CCDCOE	Co-operative Cyber Defence Centre of Excellence
CERT	Computer emergency response team
CERT-EU	EU computer emergency response team
CFSP	Common Foreign and Security Policy
CIP	Critical infrastructure protection
CIIP	Critical information infrastructure protection
COM	Commission Communication
CNO	Computer network operations
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
DDoS	Distributed denial of service
DG	Directorate General
DG Connect	Directorate General for Communications Networks, Content and Technology
DG GROWTH	Directorate General for the Internal Market, Industry, Entrepreneurship and SMEs
DG HOME	Directorate General for Migration and Home Affairs
DG MARKT	Directorate General for the Internal Market and Services*
DNS	Domain name system
EAEC	European Atomic Energy Community
EC3	European Cyber-Crime Centre
ECSC	European Coal and Steel Community
EDA	European Defence Agency
EDC	European Defence Community (proposed)
EEA	European Economic Area
EEAS	European External Action Service
EEC	European Economic Community
ENISA	European Network and Information Security Agency
EPC	European political co-operation
EU	European Union
EUCSS	Cyber Security Strategy of the European Union
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
Eurojust	European Union Judicial Co-operation Unit
EUR-Lex	Access to European Union Law database

Europol	European Police Office
FoP	Friends of the Presidency
HI	Historical institutionalism
HR	High Representative of the Union for Foreign Affairs and Security Policy
HTCC	High-tech Crime Centre
ICANN	Internet Corporation for Assigned Names and Numbers
ICDS	International Centre for Defence and Security
ICT	Information and communications technology
IGC	Intergovernmental conference
IR	International relations
ISP	Internet service provider
IT	Information Technology
JHA	Justice and Home Affairs
NATO	North Atlantic Treaty Organisation
NIS	Network and information security
PD	Path Dependency
QMV	Qualified Majority Voting
RCI	Rational choice institutionalism
Retcon	Retroactive continuity
SDA	Security and Defence Agenda
SEA	Single European Act
SI	Sociological institutionalism
SME	Small and medium sized enterprises
SMP	Single Market Programme
SSIS	Strategy for a Secure Information Society
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
The Council	The Council of the European Union
UACES	Universities Association for Contemporary European Studies
UK	United Kingdom
USA	United States
W3C	World Wide Web Consortium
*	No longer active

Dedication

For my wife, Shona

And our daughter, Ädeline

and

For my mother and father, Betty and Peter

"Institutions persist through time, organising politics into something more than a seamless flow of activities and events."

(Orren and Skowronek, 1996, p. 111)

"Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators in every nation…A graphic representation of data from the banks of every computer in the human system. Unthinkable complexity."

(Gibson, 1984, p. 67)

Chapter 1 | Introduction

1.1. Introduction

On the 17th May 2016, the Council of the European Union formally adopted new rules to enhance cyber security across the EU. *Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union* (European Parliament & Council of The European Union, 2016) is intended to "support and facilitate strategic co-operation between Member States" (European Commission, 2016a). The Directive lays down security obligations for operators in critical sectors (such as energy, transport, health and finance) and for digital service providers (online marketplaces, search engines and cloud services). In addition, each EU Member State will for the first time be required to ensure that they are properly equipped to tackle cyber security incidents. The obligations placed on them include designating one or more national authorities, establishing a strategy for dealing with cyber threats and setting up a Computer Security Incident Response Team (CSIRT) (European Commission, 2016a).

How the EU reached this position is a long and fascinating process. EU cyber security policy evolved during a time when the world became more digitally connected and in turn more digitally vulnerable. The need for the EU to become more involved in cyber security is not difficult to comprehend when it is placed in the context of the major cyber security incidents which have occurred in recent years. The cyber-attacks on Estonia in 2007, the discovery of Stuxnet in 2010 (Farwell and Rohozinski, 2011, p. 23) and the release of classified data by National Security Agency (NSA) contractor Edward Snowden (Greenwald and MacAskill, 2013) increased political and academic interest in cyber security as a policy sector. The response of the EU has not been to deepen the integration

of the Union, but to oversee better co-ordination between its members and to focus on particular forms and types of security threat.

The *Cyber Security Strategy of the European Union* (EUCSS) is the exemplar of this policy and approach. Published in 2013, it promotes a pragmatic, socio-economic approach to cyber security challenges. The EU's policy is to ensure the economic viability of the internal market and associated digital infrastructures and networks. This is to be achieved by prioritising the functionality of systems reliant on those digital networks (European Commission, 2013a, p. 5). This resilience-based approach is to be achieved by promoting co-operation between interested entities rather than by concentrating on national security or defence provisions and military capabilities (European Commission, 2016b).

The EU's socio-economic approach is a contrast to the strategies of other international actors. States such as the United States (US), the United Kingdom (UK), Estonia and Georgia have prioritised the protection of digital networks and assets in a similar, socio-economic manner to the EU. However, in response to important international cyber incidents, they have also included military, defence, or national security-focused solutions in their strategies, often with offensive capabilities. The UK categorises cyber security as a Tier 1 national security risk alongside terrorism, major natural disasters and international military crises (United Kingdom, 2010, p. 27). The US cites a secure cyberspace as being one of its top national security priorities (USA, 2010, p. 4). The US also retains the right to respond to a cyber incident with all the diplomatic, informational, economic and military tools at its disposal, implying the use of kinetic weapons (USA, 2011a, p. 14).

The EU's approach stands apart from these defence-oriented strategies by focussing *solely* on socio-economic, criminal justice aspects of cyber security. It acts as a counter to the hype, exaggeration and threat inflation common to much academic and policy analysis of cyber threats (Hansen and Nissenbaum, 2009, p. 1164). Understanding *why* the EU has developed and continued to concentrate on this socio-economic approach to cyber security has not been explored in any great depth in existing literature. This poses an interesting puzzle which this thesis seeks to address: why, when faced with the same challenges as other international actors and states, has the EU developed and continued to follow a socio-economic path of engagement?

To address this puzzle, the thesis will focus on internal EU processes, rather than conduct an examination of external influences such as the actions of NATO and the EU's relations with that alliance. There are three reasons for this internal focus. First, as introduced in

Section 1.6 of this chapter, and as explored in detail in Chapter 4, the EU can be considered an international actor in its own right. It has an international presence as well as the capabilities and opportunities to engage with cyber security issues (Bretherton and Vogler, 2006, pp. 24–35) It is therefore of benefit to academic and political commentators to examine the response of that actor to an important security challenge. Second, the thesis seeks to examine and understand EU policy-making processes. Such processes are an integral, internal part of the way the EU functions. This gives any examination of policy-making an internal focus. Finally, as stated in the previous paragraph, the EU was exposed to the same external forces and events in cyber security (the 2007 Estonian attacks, the discovery of Stuxnet inter alia). However, the EU chose a different path to other actors. If the external forces were the same for all actors, then it must have been something internal that made the difference.

There are caveats to such an internal focus, however. Concentrating an analysis on internal policy-making processes may at first appear to exclude external dynamics, or to infer that such dynamics played no role in EU policy-making. However, as will be shown in Chapters 8 and 9, the role of external events is taken into consideration in this thesis through a detailed examination of the EU's response to those events and why the EU chose that response.

Throughout the thesis, the argument will be made that EU policy and its continuation stems from an interplay of institutional and ideational influences. Specifically, the thesis will argue that Union competences interact with a policy discourse predicated upon five key ideational elements – trust in digital systems, the protection of rights, ensuring economic viability, tackling cyber-crime and achieving these through facilitating co-operation. These ideational elements both inform a socio-economic policy discourse and facilitate its continuity. A result of this interaction is that the direction of EU policy was able to continue unchanged between 1985 and 2013. This continuity was maintained even in the face of major events and crises. From a theoretical perspective, this has implications for certain aspects of historical institutionalism, in particular Krasner's (1984, p. 240) models of punctuated equilibrium. Instead of generating policy change, major events and crises led to policy continuity.

This opening chapter will explore these puzzles in more depth and lay out the approach that the thesis takes as a whole. The chapter is divided into five sections. Section 2, which immediately follows this introduction, will set out the focus of the thesis, the research

question the thesis will answer as well as the rationale for engaging in this research topic. The section will also position the thesis in current academic literature pertinent to this topic. Section 3 explores the theoretical framework in which the thesis will be positioned: historical institutionalism (HI). It examines how the selection of HI informed the development of the specific research question this thesis will answer.

The analytical and methodological framework employed in answering the research question is examined in Section 4. The section sets out the research and data collection methods used to gather information for examination in the empirical chapters. Section 5 clarifies important definitions and terminology which will be used throughout the thesis while Section 6 outlines the thesis's structure and summarises the main findings.

In addition to explaining the argument and methodology, this chapter also sets out the original contributions to scholarship made in this thesis. There are a number of such contributions. The thesis examines an under-researched area of EU policy, namely cyber security. In addition, it seeks to explain *why* the EU adopted a particular policy approach, and not just *what* that approach is. The goal of the thesis is more than simply providing an historical narrative showing how the EU got to its policy choice in 2013. By examining and understanding the processes, influences and dynamics involved in the development of the EU's cyber security policy, why the EU adopted the approach it did can be discerned, a contribution of greater value to academic and political discussions of EU policy.

The thesis also examines the role of 'abstract' institutions in EU policy-making, rather than focussing on the actions of existent, 'bricks-and-mortar' organisations. To facilitate this analysis, two methodological contributions are made: the development of a conceptual content analysis technique and a new model for determining the "actorness" of composite entities. From a theoretical perspective, applying historical institutionalism to cyber security is itself an original endeavour. Although cyber security has been examined as a research topic it has not previously been subjected to an HI analysis. Finally, as will be shown in the empirical chapters of this thesis, EU cyber security policy does not conform to models of punctuated equilibrium. These models stipulate that policy paths continue until a major event, crisis or other critical juncture causes policy change. In the case of EU cyber security policy, these critical junctures served to maintain continuity. This means that punctuated equilibrium is more flexible than it can at first appear, and can be used to explain policy continuity as well as policy change.

1.2. Focus of thesis, rationale and placement in the literature

Cyber security has received less academic attention than other areas of EU policy. Those analyses which have been carried out are either internal reports (Klimburg and Tiirmaa-Klaar, 2011), research commissioned by the EU's institutions (Cornish, 2009) or publications intended to "explain the evolution of the EU governance system for cyber security" with a focus on resilience (Christou, 2016, p. 3). Current studies therefore focus on *how* the EU seeks to achieve cyber security (Christou, 2016; Sliwinski, 2014). They have not explained *why* the Union adopted its socio-economic, resilience-based approach, or why this approach has been so unchanging. By examining this phenomenon, this research will make a contribution to the body of literature relating to EU policy and policy-making. Specifically, the thesis will investigate whether or not certain institutional arrangements have led to the development and continuity of the EU's approach to cyber security. This focus raises the specific research question the thesis will seek to answer: *have institutions and institutional arrangements led the EU to develop and continue with a socio-economic approach to cyber security?*

The first key finding of this research is that the EU has a specific policy discourse in cyber security. As will be examined in detail in Chapter 5 this policy discourse is derived from a socio-economic standpoint. It concentrates on ensuring the availability of the commercial and social opportunities provided by networked communications. The internet, and information and communications technology (ICT) in general, are treated as tools for economic growth, free speech and the exercise of fundamental rights (European Commission, 2013a, p. 2). Cyberspace is considered a vital component of the EU's Single Market and the economic wellbeing of the Union and its citizens. The EU's priorities are therefore to ensure that European society can use the online domain to its full potential but in a safe and secure manner, and that no-one is denied access to the opportunities cyberspace can provide. To achieve these goals, the EU seeks to position itself as a facilitator of co-operation and information exchange.

This discourse is exemplified in the EUCSS of 2013. However, the discourse is not an *ad hoc* construct. This thesis will demonstrate that the discourse developed over a period of 28 years, specifically between 1985 and 2013. Most importantly, it is shown in this thesis that this discourse did not alter during those 28 years, despite significant institutional change within the EU and the occurrence of major cyber security events around the world.

In response to these events, other actors changed their approach and added national security and defence concepts to their own strategies. The EU continued on its socio-economic path. This combination of the development of a socio-economic discourse, and the continuity of that discourse despite the occurrence of major events, is the subject of this thesis.

In addition to examining why the EU adopted and maintained its approach, this research is important because it focusses on the influence of more abstract institutional dynamics. Institutional analyses undertaken to date have concentrated on the role played by existent organisational bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN), the World Wide Web Consortium (W3C) and the NATO Co-operative Cyber Defence Centre of Excellence (CCDCOE) (Choucri et al., 2014). These existent institutions are also different types of bodies to the EU. They serve very specific, technical purposes. ICANN and the W3C focus on promoting and maintaining standardisation in the use and development of the Internet. The CCDCOE is a think tank which focusses on researching cyber conflict. None of these bodies, however, have as broad a remit as the EU. Yet despite its unique organisational structure, legislative mandate, international economic position and promotion of the digital single market, the EU has, surprisingly, been overlooked in analyses of cyber security.

Taking this significant institutional context into account, this thesis will examine the influence of ***abstract institutions*** on the process of cyber security policy development. Institutions are understood in this thesis as the rules, norms, standard operating procedures and common practices in which policy is made. As such, the EU's system of competences is the institution on which this thesis will focus. The effect of abstract institutional constructs such as policy norms, principles and the rules governing actor interaction is also comparatively under-researched in cyber security. This is a second gap which this thesis will help to fill and in so doing aim to contribute to a better understanding of EU policy-making processes.

It is important to establish at this point that the thesis will examine the *influence* of institutions and institutional arrangements, rather than their *impact*. This is because the term "impact" means that there has been a noticeable change as a result of a phenomenon. If something has an "influence" it can effect either a specific change or reinforce continuity. "Influence" is therefore a more accurate, nuanced word to use in the context of the relationship between Union competences and cyber security.

1.3. Rationale for Applying Historical Institutionalism to EU Cyber Security Policy

The question for this thesis indicates that institutionalist approaches to social research would be the most apposite. The choice of theoretical framework for this thesis required greater consideration, however. As will be examined in Chapter 2, there is a rich heritage of theoretical approaches to the study of the European Union. Although these range from gender studies to critical approaches (Wiener and Diez, 2009), analyses of the EU tend to favour either neofunctionalism, liberal intergovernmentalism or constructivism. However, an issue arises with the application of these theories to cyber security in the EU.

The commonly applied theories of neofunctionalism, liberal intergovernmentalism and constructivism tend to theorise on the processes of integration. This is problematic because the EUCSS states explicitly that ensuring the security of systems, networks and digital data rests with the Member States. While not an explicit rejection of integration *per se*, acknowledging the primacy of the Member States in a specific policy field is not conducive to promoting ever closer union. This means that theoretical frameworks and approaches which concentrate on deeper integration become less suited to an analysis of EU cyber security policy. Historical institutionalism (HI) was found to be the most apposite theoretical framework for this thesis because it is *not* predicated upon analyses of Union integration. The other theories are not rejected outright, but instead inform the wider HI framework of the thesis.

That framework is based around three mechanisms which characterise HI approaches to the study of social phenomena in political science. These were postulated by Pierson and Skocpol (2002, p. 3). They argue that HI analyses address substantive questions of inherent interest, take time seriously by studying sequences or tracing processes and hypothesize about the interaction of institutions and non-institutional elements. Pierson, Skocpol and Steinmo (2008, p. 118) stress that this is not a specific HI methodology *per se*, but an *approach* to the study of social phenomena. The three general, systemic mechanisms are present throughout HI scholarship although the precise application of those mechanisms may vary (Bulmer and Burch, 2001; Pierson, 1996; Skocpol, 1979). What follows here is a brief exposition of the application of those three mechanisms to this thesis.

1.3.1. Applying the mechanisms of HI

The first mechanism is that HI addresses "big, substantive questions of inherent interest" (Pierson and Skocpol, 2002, p. 3). The substantive question for this research study is to understand *why* the EU has adopted its particular socio-economic approach to cyber security and continued to apply this while other actors opted to add national security considerations to their strategies. To address this problem this thesis will conduct what Pierson and Skocpol call a study of real-world "empirical patterns [that] run counter to received academic or popular wisdom" (Pierson and Skocpol, 2002, p. 4). The patterns to be examined are the institutions and institutional arrangements pertinent to policy development. This raises a supplementary question for this thesis: which institutions are the most relevant to cyber security? Answering this will help to answer the research question by establishing which "empirical patterns", i.e. which institutional arrangements, influenced the development of the EU's socio-economic policy discourse. Data will be gathered from Union *acquis communautaire* and elite interviews to answer this.

The second of Pierson and Skocpol's mechanisms is that HI "takes time seriously" (Pierson and Skocpol, 2002, p. 3). By studying phenomena over time HI allows scholars to identify and examine hitherto unseen slow-moving processes. Combining a focus on large, substantive questions with a longitudinal approach to time enables the explanation of outcomes of interest – the social phenomena under examination – well after the emergence of key causal factors. This avoids the trap of lapsing into deterministic historical causality.

This is of particular importance to this thesis. The exercise of identifying, gathering and cataloguing relevant Union *acquis* preceding the EUCSS showed that EU cyber security has an historical component that has not been acknowledged. Political interest in this sector originated in the mid-1980s. It was founded upon the desire of the then-European Community to use all possible avenues, means, methods and instruments available to stimulate economic growth in order to exit a financial crisis. The European Community chose to promote and support the burgeoning ICT industry as one of these methods (European Commission, 1985, 1993). This concentration on utilising ICT for economic growth would over time lead to the development of a socio-economic cyber security policy. While there is an identifiable linearity to the development of policy in this sector, it is not deterministic. Employing an approach which allows for the identification and analysis of processes, rather than simple causality, avoids implying that the EU's policy was an inevitable, teleological result of its original interest in ICT.

In addition to identifying the effect of institutions on this policy area, conducting this analysis will also identify the influence of *non*-institutional drivers. This leads to a second supplementary question for this thesis: were there other forces at work – particularly ideational or catalytic elements – which inform policy choices? Particular ideas or important external events can act as drivers which push policy outcomes in particular directions. Examining such drivers will facilitate the identification of specific causal mechanisms not normally accounted for in analyses of EU policy-making (Checkel and Moravcsik, 2001, p. 221).

The application of Pierson and Skocpol's (2002, p. 3) third characteristic of HI – that it "analyses macro contexts and hypothesises about the combined effects of institutions and processes" – leads to a third supplementary question this thesis will seek to answer: did an *interplay* between institutional and non-institutional policy drivers also have an influence on the reasons why the EU developed and continued with its socio-economic cyber security discourse? The thesis will study whether institutions and non-institutional elements operated independently of one another or in conjunction in influencing policy choice.

This establishes two tasks which must be undertaken in this thesis in order to answer the primary research question. First, the institutional and non-institutional dynamics pertinent to cyber security must be identified. Second, the interaction of these two elements must be analysed. Completing these tasks fulfils a core function of historical institutionalism itself. As Thelen and Steinmo (1992, p. 13) state, the purpose of institutionalism "is to demonstrate the relationships and interactions among a variety of [elements] in a way that reflects the complexity of real political interactions". To fully understand a particular social phenomenon, such as the development of a particular cyber security policy, the interactions of the relevant elements must be examined.

There are precedents for such an approach to the study of social phenomena. Hall (1992, p. 109) argued that the adoption of a monetarist economic policy by the UK government in the 1970s was not the only possible policy option available in response to the recession of the time. A continuation of Keynesian economic principles – the prevailing economic system of the period – was a viable option. This led to the question: why did the UK government change to monetarism? For Hall, the answer was to be found in competing social interests combining and interacting with changes in the operating procedures of financial markets. This interaction put pressure on British policy-makers to seek out

alternative economic models. A similar analytical process can be undertaken when examining EU cyber security policy.

Such an analysis presents another opportunity for this thesis to contribute to current scholarship. Examining the nature of the relationship between institutional and non-institutional drivers enables a model for explaining actor behaviour to be developed. That model is predicated upon particular configurations of those drivers and can be applied to any research scenario where actor behaviour diverges from the prevailing narrative. There are three possible theories to explain why the EU opted to develop and continue policy X while others opted to add policy Y. One is that the institutional architecture of the EU influenced the Union's approach to cyber security. A second is that the EU's response was not the result of institutional drivers at all, but non-institutional elements such as socio-economic policy ideas. A third potential model is that the EU's policy choice was not the result of institutional or non-institutional drivers alone, but a combination of the two. This thesis can help to identify not only which of the three explanatory theories was in effect, but also the specific policy choices which account for the divergences. By providing and exploring such models this thesis can make a substantive contribution to the study of international organisations such as the EU as well as the field of international relations.

1.4. Analytical Approach and Methodology: Data Sources and Analytical Techniques

Data analysed in this thesis was drawn from two source types. These were primary literature in the form of EU *acquis communautaire* and elite interviews carried out with Union functionaries, academics and industry specialists in the field of cyber security[1]. While the methodology will be set out in detail in Chapter 3, it is beneficial to set out a number of points here. The first is the clarification of what will be considered *acquis communautaire* in this thesis. According to the EU, the *acquis* is

> the body of common rights and obligations that is binding on all the EU Member States. It is constantly evolving and comprises:
>
> - the content, principles and political objectives of the Treaties;
> - legislation adopted pursuant to the Treaties and the case law of the Court of Justice;
> - declarations and resolutions adopted by the Union;
> - instruments under the Common Foreign and Security Policy;

[1] See Appendix 10 for a complete list of referable interview participants

- international agreements concluded by the Union and those entered into by the Member States among themselves within the sphere of the Union's activities. (European Union, n.d.)

This thesis adopts the position that Commission Communications – the majority of the EU's policy pronouncements and publications – also form an integral part of the *acquis*. This is because these Communications comprise not only proposals for legislation but also "declarations and resolutions adopted by the Union" as defined by the EU itself (European Union, n.d.). Strategy documents such as the EUCSS, a Commission Communication, are required to be considered by the Parliament and approved by either the Council of the European Union or the European Council. A set of Conclusions approved by the Council of the European Union on 25 June 2013 formally approved the EUCSS as representative of the European Union's position on cyber security (Council of The European Union, 2013a). Once this approval and adoption was confirmed, the EUCSS, a Commission Communication, became a part of Union *acquis communautaire*.

In addition to using primary literature it was necessary to gather data from elite interviews and combine the information gathered. A study of policy-making in any sector of the EU's purview cannot rely on either the *acquis* or interviews alone. Research into any EU policy sector must analyse primary documentation setting out that policy, i.e. the EU's *acquis*. That *acquis*, however, is the end point of a developmental process, a final product which offers little to no insights into its formation. To study that *process*, data must be sought elsewhere. The functionaries and bureaucrats personally involved in the development of policy are invaluable sources of information for this aspect. Union *acquis* and elite interviews are therefore mutually complementary in a study of this nature. One source provides details of the policy itself, while the other provides insights on the policy's development.

A methodological problem was encountered when combining data from two different source types. Separate research methodologies and techniques are applied to interviews and primary literature (Bryman, 2008; Berg, 2004; Hycner, 1985). Content analyses are more often applied to literature sources, while discourse analysis techniques are applied to interviews. Because both source types needed to be used in this study, a modified form of content analysis was developed specifically for this thesis. The modification blended both qualitative and quantitative elements from two current research approaches. A toolkit for the analysis of interviews was derived from Hycner (1985, pp. 280–294), while Berg

(2004, pp. 241–242) posited counting units of meaning rather than numbers of words, as would be the case in a standard, quantitative content analysis.

As will be examined in greater detail in Chapter 3, core elements of both of these methodologies were blended to form a "Hycner-Berg" model of *conceptual* content analysis. Because it drew on techniques for analysing *both* interviews and literature, the modified toolkit meant that the same methodological technique for data extraction could be effectively applied to both source types. This greatly facilitated ensuring data validity, replicability and reliability. Finally, the modified analysis was conducted using NVivo computer-assisted qualitative data analysis software (CAQDAS) to help maintain data validity and reliability.

While there were certain limitations to using both literature and interview data which needed to be mitigated using the methods outlined above, there were two distinct advantages for using these source types. One important advantage was that this method provided opportunities for triangulating findings. Data provided by academics and sector specialists were used to corroborate or challenge findings derived from both *acquis* and EU functionary interviews. Interviews with academic specialists are important because they are not a part of the EU's structure. They are able to provide more objective viewpoints and analyses of Union action.

The second advantage was that the exercise of collecting and analysing Union *acquis* relevant to this thesis provided a period of time on which to focus. The end point of the analysis is the publication of the EU's *Cyber Security Strategy* in February of 2013. This is because that Strategy is the culmination of a policy-making process. However, defining a starting point for the analysis was more problematic. Gathering the relevant *acquis* established that the earliest mentioning of ICT as a sector occurred in 1985 with the initiation of the internal market. This means that the period of time this thesis will examine is the 28 years between 1985 and 2013.

1.5. Definitions Employed in the Thesis

There are a number of terms which will be frequently used in this thesis and which merit clarification. As set out in the overview of the methodology, one such term is the *acquis communautaire*. When referring to Union *acquis*, this thesis uses the term to include Commission Communications as well as Treaties, legislation, Council Conclusions and international agreements.

There are three further terms which require elaboration of the manner in which they will be used in this thesis: “cyber security”, “European Union” and “timescape.”

1.5.1. Defining Cyber Security

International policy, legislation and regulation in cyber security suffers from a lack of consistently applied terminology (Kruger, 2012). EU policy and *acquis* is no different. “Cyber security” is used interchangeably and synonymously with other terms such as “network and information security” (NIS) or online safety. This is despite the fact that much EU *acquis* uses “NIS” in specific contexts.

Despite this, the EU offers a definition of “cyber security” in the EUCSS:

> The safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein. (European Commission, 2013a, p. 3)

For efficiency and consistency, this thesis will employ the EU’s definition but expand it to refer to the full range of issues relating to online safety, software and hardware integrity and criminal and state-sponsored malicious activity. The term will therefore be used as a generic, umbrella definition to cover the broad spectrum of cyber security concerns ranging from credit card fraud, identity theft and protection of privacy, to corporate espionage and state-sponsored hacks.

1.5.2. “European Union” or “European Community”?

As set out in Section 4 above, this thesis will examine cyber security policy development between 1985 and 2013. During this time, the EU underwent three separate transformations and was known by different names. In 1985 it was still operating under the terms of the Treaty of Brussels of 1967 which created a single Commission and single Council to serve three “communities”. These were the European Economic Community (EEC), the European Atomic Energy Community (EAEC) and the European Coal and Steel Community ECSC) (Europa, n.d.). There was at the time no single political body, but rather a composite entity comprising three separate organisations managed by a single Council.

This system continued through the 1980s and early 1990s. This is significant because it means that interest in ICT began *before* the creation of the European Union. That creation

occurred in 1993 with the entry into force of the Treaty of Maastricht. As will be examined in Chapter 6, that Treaty had an important influence on EU policy-making in general and on cyber security in particular, due to the creation of a single political entity made up of three separate pillars. This system continued until the entry into force of the Treaty of Lisbon in 2009 which abolished the three pillars and created a single political entity with a unified legal personality.

As a result of these changes, since 2009 it has become academic convention to refer to all the historic iterations and guises prior to 2009 as the "European Union", irrespective of the time period under examination. This thesis will adopt this academic convention in order to reduce the potential for confusion and to aid clarity. This exercise of applying modern terms to historic issues is known as "retroactive continuity".

1.5.2.1. Retroactive Continuity: Applying modern terms to historic concepts

Retroactive continuity, or "retconning", refers to the process of amending past narratives to avoid inconsistencies with modern ones (Blundell et al., 2010, p. 4; Martin, 2014, p. 5). Although a device common in fiction writing, it is appropriate for use in an historical institutionalist analysis due to modern terms being used to describe long-standing issues.

Retroactive continuity is particularly relevant to this study because the issues which come under the umbrella term "cyber security" are not modern. Unauthorised access and intrusions into networked systems or the theft and manipulation of digital data have been security concerns since the earliest use of networked ICT (Healey, 2013). The issue here is that none of these early security concerns were labelled "cyber security". Instead they are being retroactively included in a modern interpretation of the concept. This has occurred in both data sources used for this research: *acquis* and interviews. In the EU context the term "cyber security" did not appear in Union *acquis* until 2002. This is 18 years *after* the commencement of EU interest in the sector. The preferred term in the earliest periods of Union interest in this sector was "online safety" from illegal and harmful content (European Commission, 1996a). By 2001 policy-makers had adopted "network and information security" as a term broad enough to cover issues relating to online safety[2]. These included fraud, child exploitation and copyright infringement.

[2] This will be examined in Chapter 5 on the EU's cyber security discourse

The potential limitations of retroactive continuity can be mitigated by acknowledging the existence of this device and accepting that, in certain circumstances, it is unavoidable in HI research. This thesis aims to understand and explain a long-term policy-making process in a sector which was only recently defined. In order to examine and understand the development of any policy discourse it is necessary to identify concepts or ideas and trace them to their origin. Where there is an historic component, achieving this inevitably involves applying modern terms to historic concepts. It is necessary to use a form of mitigated or controlled retconning in order to carry out an analysis. Applying the EU's definition to all instances of online safety or NIS between 1985 and 2013[3] necessarily involves retconning. Acknowledging this device mitigates its effect on the validity and reliability of the analysis.

1.5.3. "Timescape" versus "timeframe"

The final clarification relates to the terminology used to describe the 28-year period under examination. Instead of using terms such as "timeframes" or "chronologies" this thesis will adopt the term "timescape". Bulmer (2009, p. 307) describes a timescape as "the manner in which time is institutionalised in a political system along the polity, political and policy dimensions". This conceptualisation facilitates HI analyses such as this thesis because it looks at political and social processes *in* time rather than *over* time.

This is an important distinction. A timescape differs from concepts such as a "timeframe", "timescale" or "chronology" because it is not concerned with purely historical analyses which focus on the influence of the past on the present (Meyer-Sahling and Goetz, 2009, p. 181). A timescape infers that a greater importance has been placed on the timing of social phenomena – when they occurred in a sequence of events – rather than simply placing them in an historical chronology.

The notion of a timescape is therefore invaluable to conducting a study of EU policy-making. This is because this topic is a developmental process and not an *ad hoc* creation or a deterministic product. This is particularly valuable for this thesis given that it seeks to explain a particular social phenomenon – the EU's cyber security discourse – but endeavours to do so without lapsing into historical causality[4]. As will be examined in greater detail in Chapters 5 and 6, the institution of greatest influence in EU cyber security was formalised *after* the initiation of the policy discourse itself. The timing of these two

[3] As was examined in Section 1.5.1. of this chapter.
[4] As described in Section 1.3.

elements is significant, but that significance would have been lost had a simple historical analysis been carried out.

1.6. Thesis outline and main findings

The thesis is divided into ten chapters including this introduction. Chapter 2 provides a critical review of current academic literature in two areas of scholarship. The first relates specifically to the literature on the EU and cyber security. Compared with other policy areas in the EU there is a relatively small body of scholarship to draw upon. This is because Union cyber security policy remains a developing area of academic study. The main debates surround measures undertaken to combat policy fragmentation prior to 2013, such as fostering co-operation between entities involved in cyber security.

The second area of scholarship reviewed in Chapter 2 examines the various theoretical frameworks most prominent in analyses of EU policy-making in general. Neofunctionalism, liberal intergovernmentalism, constructivism and institutionalism are evaluated as possible frameworks for this thesis. The reasons for selecting HI are then set out.

Chapter 3 explains the research methodology employed to identify and gather data sources, extract and analyse data. As set out in Section 1.4 above, a mixed-methods approach combining quantitative and qualitative analytical techniques was employed to gather data on how institutional processes informed or influenced policy choices.

Chapter 4 follows on from the methodology by setting out the HI mechanisms which form the theoretical framework to be employed in the analysis. The chapter will also clarify two important aspects of an HI analysis: which institutions and which actors will be examined. The thesis adopts Hall's (1992, p. 96) definition of institutions as formal rules, standard operating procedures and customary practices which influence actor behaviour and policy choice. Given this position, the standard operating procedures and rules which most affect EU policy-making are the Union's competences. This is because the competences specify in which policy sectors, and to what degree, the EU can become involved. The clarification of Union competence and the institution of greatest influence is the first of the thesis's three main findings. The influence of competence on the EU's cyber security policy-making process will be examined in the empirical analysis.

The actors for the study are the seven formal entities of the EU which operate within the setting of Union competences. These are the European Council, the Commission, the

Council of the European Union, the European Parliament, the Central Bank, the Court of Justice and the Court of Auditors. This position is justified by developing a model of "actorness" predicated upon a combination of Scharpf's (1997, p. 52) definition of "composite actors" with Bretherton and Vogler's (2006, pp. 24–29) conceptualisation of "actorness". This Scharpf-Bretherton-Vogler conceptualisation enables these seven principle bodies to be classified as actors. The development of this new model is one of the main contributions to scholarship this thesis makes. Finally, Chapter 4 will outline why four of these actors, namely the Council of the European Union, European Council, Parliament and Commission, are more important for this thesis than others such as the Central Bank or Court of Auditors.

Chapters 5, 6, 7, 8 and 9 comprise the empirical section of the thesis. Chapter 5 sets out the EU's cyber security discourse. The clarification of the existence of a specific policy discourse is the second of the thesis's three main findings. After adopting Gasper and Apthorpe's (1996, p. 2) definition of the term "discourse" as the manner in which particular issues are framed, the EU's cyber security discourse is identified in its *acquis communautaire*. Setting out and clarifying the EU's discourse in cyber security is important for a number of reasons. That framing differs from the prevailing narrative of international cyber security policy because it is *purely* socio-economic in nature. Other approaches have included national security considerations. Clearly setting out the discourse also facilitates the analysis of this approach. This exercise also demonstrates that the discourse was not an *ad hoc* policy, created solely for the EUCSS of 2013. Instead, as will be demonstrated in Chapter 5, it was developed and constructed between 1985 and 2013, clearly providing a timescape for analysis.

Finally, the chapter demonstrates that that discourse construction was predicated upon five core ideational elements which endured throughout the policy-making timescape and underpinned the EUCSS itself. These five elements are economic maximisation, ensuring trust in digital technologies, tackling cyber-crime, protecting fundamental rights and fostering co-operation. The elements are so pronounced that they constitute core themes to be examined throughout the empirical chapters of the thesis.

Chapter 6 examines the years between 1985 and 2001 and focusses on the initiation of core path dependencies. Path dependency is an important aspect of historical institutionalism because it explains how decisions made early in a process continue to have an influence in subsequent periods. The chapter explores how the five ideational elements of the EU's

cyber security discourse, elements which would endure throughout the 28 year timescape, were established and became path dependencies. Crucially, the chapter explores how these policy paths were laid down *before* Union competences were formalised.

The stabilisation of those early policy paths is explored in Chapter 7. This occurred in the years between 2001 and 2006. The mechanisms of path dependency mean that once a policy choice has been made it enters a period of stasis and consolidation. The chapter will demonstrate that, in the case of EU cyber security, that consolidation is manifested by the initiation of specific agencies which were tasked with operationalising core aspects of policy. The consolidation process culminated in 2006 with the publication of a Commission Communication promoting the development of a secure information society.

Chapters 8 and 9 examine the policy-making process's exposure to institutional stresses between 2007 and 2013, the final period of time in the analysis. The purpose of this exercise is to demonstrate the resilience of policy paths and the EU's underlying discourse to major exogenous and endogenous events or punctuation points. This resilience is examined in three case studies, representing three different types of punctuation.

Chapter 8 examines two case studies exogenous to the EU in order to study the effect of external events on Union cyber security policy. The first case study is the cyber-attack on Estonia in 2007. The chapter examines how the Union responded to that incident. Due to restricted competence in foreign and security affairs the EU required a creative interpretation of the attack in order to be able to respond effectively. The precise nature of that interpretation and response is explored in the first section of the chapter.

The second case study is the influence of a major event in which the Union had much greater competence. In 2008 the EU was caught up in the global financial crisis which began in the US sub-prime mortgage market. In order to boost economic growth the ICT industry was once again targeted for specific attention, a move reminiscent of the late 1980s. The main difference was that by 2008 the digital domain had become critical to the ongoing functionality of other physical infrastructures. It needed to be secure and resilient against future downturns and crises in order to ensure that economic opportunities could be exploited and trust in digital commerce maintained. Both of these events served to entrench established policy paths, rather than effect any change in the EU's approach to cyber security.

Chapter 9 examines the final case study: the influence of the Treaty of Lisbon on cyber security policy development. In reshaping the architecture of the Union itself, most notably by abolishing the Pillar structure established by the Maastricht Treaty in 1992, the Treaty of Lisbon streamlined the EU's policy-making processes. This enabled formal co-operation between functionaries previously separated by the Pillars and led to the development of a holistic EU cyber security policy. In short, without the Treaty of Lisbon, the EUCSS would not have come about.

Throughout the examination of these case studies, the argument will be made that EU competences were the institutional framework of greatest influence in cyber security policy. While the EU's original, initial interest and discourse in ICT was socio-economic, Union competences created a framework in which that discourse could not deviate from this initial position. The empirical chapters will also present the argument that these institutional stresses entrenched the EU's cyber security discourse, rather than led to change. This means that the incidents did not influence cyber security policy in a manner to be expected by HI approaches, notably punctuated equilibrium and path dependency. Punctuated equilibrium is an HI mechanism for explaining policy change whereby choices remain in place until a major event shifts that policy onto a new path. The opposite effect occurred here. Rather than cause change, the three punctuation points served to entrench established policy paths and encourage their continuity. The paradoxical resilience of EU cyber security policy to those three critical junctures will be explored in these chapters. EU cyber security's paradoxical lack of conformity to punctuated equilibrium is the third main finding of this thesis.

Chapter 10 concludes the thesis. It summarises the main findings of the research and highlights a number of implications for academics and EU practitioners. The chapter also sets out the contributions the thesis makes to scholarship on the EU and HI as well as identifying potential avenues for further research.

Applying HI mechanisms to EU cyber security is itself an original endeavour. This research will therefore make a substantive contribution to the study of EU policy-making by applying HI methods and tools to an under-research policy area. In addition, the model of institution and idea interaction developed in this thesis can be applied not just to the EU's approach to cyber security, but to other policy areas where there is a divergence from prevailing policy and academic narratives. As a result, this research will make a

substantive contribution not just to academic studies of the European Union but also to historical institutionalist scholarship.

Chapter 2 | Literature Review: The EU and Cyber Security – Debates and Theory

2.1. Introduction

Academic studies of EU cyber security are limited. Nevertheless, available scholarship demonstrates a small but dynamic research agenda, covering topics as diverse as cyberbullying, online criminal activity and the use of ICT in industry. Current literature has not, however, examined the development and evolution of the field within the context of the EU's policy-making process. This is important because EU policy diverges from academic and political cyber security narratives. It advocates a purely socio-economic, criminal justice approach to cyber threats without any military or defence capacity. Other actors include national security-oriented solutions. To date, why this is the case is a question which has not been asked in current academic studies. This is an important omission which this thesis addresses. To fully understand a system – such as a policy-making process – it is not enough to understand how that system operates and produces results. One must understand *why* the system functions the way it does. This thesis seeks to address this gap, a goal which positions the thesis as an examination of EU policy-making, with cyber security as the vector or lens for this analysis.

In reviewing academic literature relevant to this thesis, the chapter will first examine the small corpus of literature on EU cyber security policy. There are two themes within that body of research. The first is the recognition of a fragmented EU policy in this field. Because of the range of policy sectors in which cyber security plays a part, prior to 2013 there was no overarching, holistic strategy for dealing with cyber security in all its guises. There has consequently been no overarching, holistic academic study of cyber security in the EU context. This is an important gap in academic literature because an environment where there exists a fragmented policy approach and a range of policy instruments is not one conducive to policy continuity. This makes a long-term, continuous socio-economic approach to cyber security, such as that of the EU, even more surprising.

The second theme in current scholarship is the acknowledgment of co-operation as a crucial component of EU policy in this sector. Despite the fragmentation of policies and approaches, the overall tenor of EU policy is geared towards facilitating and promoting co-operation between actors.

The recognition of co-operation as a crucial element of EU cyber security is important for this thesis's research question because, unlike fragmentation, co-operation *is* conducive to policy continuity. This is especially the case in the EU context. As will be shown in Chapter 5, co-operation is one of five core ideational elements which are present throughout the 28 year timescape of cyber security policy development. Christou (2016) goes so far as to say that facilitating co-operation is the EU's purpose as an actor in international cyber security. However, as will be shown in this literature review, he does not say *why* this should be the case. This is a common issue with analyses of EU cyber policy. There is a heavy focus on *what* the EU is doing in this sector and *how* it goes about this, but very little analysis of *why* this policy approach was chosen. This is the second gap in the literature which this thesis addresses.

The chapter will also present the theoretical framework used in this research. To date there have been limited attempts to conduct theoretically grounded analyses of EU cyber security policy. This is a third gap in the literature which this research will address. The section will conduct a comparison of four of the most prominent theoretical approaches to EU studies: neofunctionalism, intergovernmentalism, constructivism and institutionalism. This comparison will show that the first three traditions are less suitable for a study of cyber security than institutionalism. While these traditions can inform a study of cyber security policy development, neofunctionalist, intergovernmentalist and constructivist approaches tend to focus analyses on the processes of integration. This makes them less suitable for this thesis due to the EU's position that cyber security is largely the responsibility of the Member States. The chapter will close by demonstrating that for this reason institutionalism, particularly the historical variant, is the most apposite framework for this study due to its comparatively reduced concentration on integration. HI is also apposite because policy-making in the EU is not a speedy process. It takes years for proposals to be developed, debated and agreed upon. As shown by this literature review, cyber security also has a long pedigree. HI lends itself to such a study by taking into account processes being carried out *over time*. This research will therefore make a second substantive contribution to the wider literature on the EU; it will conduct an HI analysis of a policy sector not previously subjected to such an examination.

The chapter is divided into four sections, in which the three specific gaps in scholarship are addressed. The second section of this chapter reviews the small corpus of literature on EU cyber security policy. The third section of the chapter will examine four key theoretical

approaches to the study of the EU, before explaining why historical institutionalism was selected as the framework for this thesis. A fourth section concludes the chapter.

2.2. Academic debates

2.2.1. Fragmentation of the EU's approach

Relative to other areas of EU policy, the body of literature examining Union cyber security policy is small. This is reflected in a tendency within that scholarship towards specificity. Academic analyses address highly focused subjects, such as the relationship between EU and US intelligence agencies (Segell, 2010), the adoption of broadband Internet and its impact on regulation (Briglauer, 2014), or a balancing of security with privacy (Liberatore, 2007). A recent analysis published by the European Organisation for Security (ESO) provides a detailed breakdown of the risks and threats to critical infrastructure from cyber-crime and cyber-terrorism, and the role of public-private partnerships in addressing these (Olesen, 2016). Despite the specificity of their subject matter, what these analyses show is the wide variety of policy areas in which cyber security has an impact, a fact recognised by the EU. As one Union official stated, cyber security is like "an octopus", it is an important consideration in a huge range of policy areas (Interview, Senior Official, DG Connect, European Commission, 2014). It also highlights what is missing from that scholarship: a whole-of-sector approach to EU cyber security that takes account of the range of policy areas on which cyber security has an effect. This is an important omission.

One of the earliest works to examine EU cyber security – and one of the widest in its scope – was Crago's (1996) analysis of the relationship between fundamental rights and the developing Internet. It provides an examination not just of Union interest in this domain, but also of the capacity of the EU to temper Member States' drives to censor legitimate use of the Internet through heavy-handed regulation of "indecent material" (Crago, 1996, p. 479). Because of an uncertain capacity for the EU to exert judicial jurisdiction (Crago, 1996, p. 480) there was a tendency to employ national laws to prosecute individual users. This became problematic when those users were not nationals of the prosecuting state. The result was an issue which would become systemic in EU cyber security: a fragmented and fractured approach due to the absence of overarching, harmonising EU instruments.

This fragmentation was present in other policy areas affected by online communications. Antezana (2003) and De Werra (2002) argue that co-operation and measures to prevent copyright infringement were relatively successful by 2003. De Werra's point centres on the agreement in 1996 that the technological measures designed to circumvent copyright

should be subject to legal ramifications (De Werra, 2002, p. 3). This was particularly important given that, as Antezana (2003, p. 415) argues, "technology and the Internet have created substantial global markets in electronic commerce". The crux of the matter was that, as the technological capacity to disseminate information increased, so too did the capacity to illegally distribute content or engage in digital piracy. Broadhurst *et al* (2014, p. 3) argue that cyber-crime evolved in parallel with the "opportunities afforded by the rapid increase in the use of the Internet for e-commerce". Just as the technology to spread information and ideas, as well as the tools to protect those ideas, was being developed, so too were the means to breach that protection for criminal gain. In other words, "what one technology can do, another can generally undo" (Samuelson, 1996, p. 4).

Antezana (2003, p. 435) further argues that there was an obstacle preventing a truly harmonised approach being developed. By 2003 there was a disconnect between legitimate copyright protection, the potential revenues from increased e-commerce (forecast to $300 billion by 2003) and European Union legislation trying not to pre-empt national law-making. The need to address these three distinct aspects invariably led to conflicts of interest which fractured Union attempts to develop holistic policies. The goal was a harmonised approach to exploiting the internet for commercial purposes (Crago, 1996) with the EU as a facilitator, but this harmonisation was still a work in progress by 2003 (Antezana, 2003, p. 136).

What these analyses omit was the action taken by the EU to attempt to resolve this issue. The fragmentation of policy instruments was a recognised problem by 2002 (Council of The European Union, 2002a, p. 4). However, steps had been taken as early as 2001 to remedy this, steps not addressed in the literature. The 2001 *Proposal for a European Approach to Network and Information Security* (European Commission, 2001a) was a first attempt to draw together the disparate elements of network and information security (NIS) policy, the name by which cyber security was then known. It should be acknowledged that Antezana's focus was purely on the EU's *Internet Copyright Directive*, but given that digital piracy was a threat identified by the Union in 1996 (European Commission, 1996a, p. 3), the analytical net could easily have been cast more widely. It is a central argument of Chapter 6 of this thesis that the EU's acknowledgement of illegal and harmful content in the mid-1990s was a milestone in the development of a holistic cyber security policy, one which addressed the issues of fragmentation but which was not examined in the studies of the time.

Fragmentation affected not just specific policy sectors affected by cyber security. Dunn Cavelty (2013, p. 4) argues that it affected cyber security policy itself. According to Mendez (2005, p. 511), this was in part due to a divided bureaucratic foundation for cyber security as a policy sector, and the further division of decision-making at the centre of that bureaucracy. As Robinson (2013, p. 96) points out "understanding who talks to whom and how co-ordination and co-operation is achieved is very complex". As demonstrated in Chapter 5, decision-making in this policy area is divided between the Commission, the European Council and the Council of the European Union. Which actor is in the ascendancy depends on the nature of the issue as well as the type of decision being made.

Fragmentation clearly problematizes issues at the micro-level, such as which tools for data protection notification are most suitable (Robinson, 2013, p. 93). Fragmentation also causes problems at the macro level. If it is not clear which bodies, agencies or policy instruments do what jobs, the social goals identified by Crago – exploiting the economic opportunities of cyberspace and the Internet – become that much harder to achieve.

Specific security goals are also difficult to achieve. Bossong (2014, p. 8) argues, for example, that information-sharing networks deemed critical for industrial resilience and counterterrorism would not "serve an important function over the medium term" due to the EU's fragmented and weak institutional basis for critical infrastructure protection. This view is supported by Boin *et al* (2014, p. 426). The ability of the EU to react to crises is adversely affected by this fragmentation. While not going so far as to say crisis management is compromised, they make the point that a lack of cohesion, harmonisation, "inter-institutional strife and cross pillar divisions tend to get worse during crises" (Boin *et al*., 2014, p. 426).

Fragmentation of policy and goals was a serious issue for EU cyber security policy regardless of whether it stemmed from a lack of centralised co-ordination at the EU level (Mendez, 2005, p. 511) or from individual Member States seeking to "develop a coherent national response to the effect of the Internet on national laws and social values" (Crago, 1996, p. 468). The problem was so acute that two internal reports commissioned by the European Parliament specifically cited policy fragmentation as an obstacle for coherent cyber security policy. Although Cornish (2009, p. 3) labelled the EU's interest in cyber security "fragmented yet developing", he argued that that interest was so fractured that

> It is difficult to identify an EU body or agency which does not have some interest or involvement in cyber-security concepts and policy on the one hand, and/or in delivery and operations on the other. (Cornish, 2009, p. 27)

By 2011 the situation had not improved. Klimburg and Tiirmaa-Klaar (2011, p. 29) argued that the EU's whole approach to the issue of cyber security was "highly fragmented".

According to the literature, systemic fragmentation has not yet been resolved, particularly in the areas of cyber-crime and the development of a market for cyber security products. From an economic perspective, Olesen (2016, p. 261) argues that the market for cyber security products and solutions also remains fragmented. This has led to a reliance on non-European cyber security products and a lack of standardisation. While Olesen does not argue that there is an inherent insecurity in such third-party products and solutions, she makes the point that there is the possibility for vulnerabilities, such as digital or software backdoors, to go unnoticed given the lack of end-to-end scrutiny of the ICT industry.

From a criminal justice perspective, Christou (2016, p. 2) argues that, while the whole EU policy towards cyber threats in general "has often been quite fragmented", the Union's approach to cyber-crime in particular still suffers from a lack of an overarching framework (Christou, 2016, p. 102). The Council of the European Union and the European Commission considered a comprehensive approach to the problem in 2001 (European Commission, 2001a). They went as far as encouraging Member States to ratify the Council of Europe Convention on Cybercrime (European Commission, 2010a, p. 2). Despite these initiatives, the EU still employs "a series of legal and regulatory instruments that overlap" (Christou, 2016, p. 136). There are moves to reduce fragmentation, such as a common breach notification process, but the lack of an overarching framework means division persists.

Carrapiço and Trauner (2013, p. 17) provide a counter to this pessimistic view of EU policy in cyber-crime by arguing that Europol has positioned itself as a central point of reference, and therefore as a force of influence on EU policy as a whole. Due to its mandate as a focal point for cyber-crime intelligence and its resources in tackling this form of activity, Europol has "been able to exert an influence beyond its narrowly defined mandate" (Carrapiço and Trauner, 2013, p. 1) and into the policy arena. However, Carrapiço and Trauner acknowledge that this role and influence is contingent on the amount and quality of data provided to Europol by the Member States. This brings into

focus a larger problem for the EU in tackling policy fragmentation: the different priorities placed on cyber-crime and cyber security by the Member States themselves.

The EUCSS makes it clear that it is the task of the Member States to deal with security risks from cyberspace (European Commission, 2013a, p. 4), meaning that responsibility for ensuring cyber security rests with them. The EUCSS also seeks to ensure a common minimum standard for security (European Commission, 2013a, p. 5). Purser (2014, p. 98,103) provides insights into how different national priorities for standardisation can be overcome by stimulating the development and implementation of industry-led standards as well as ensuring conformity. Establishing a common system of standards can help to promote information exchange and are beneficial in cross-border environments such as the Internet and cyberspace. However, establishing a common minimum standard is not the same policy goal as ensuring a common prioritisation across the 28 national governments of the Member States. This is an important facet of fragmentation, but one only rarely addressed in the literature. Kabanov (2013, p. 9) alludes to it in his comparative analysis of Russian and EU policy discourses but only in the sense that not all Member States perform the same actions with the same significance. Sarma (2016, p. 4) also infers this diverse prioritisation in her breakdown of individual UK, French and Estonian actions in cyber security within the context of EU policy. These analyses miss an opportunity, however, to examine the important question as to *why* the Member States place different levels of priority on cyber security in their national frameworks and what effect the differing national priorities have on EU cyber security as a whole. Although current studies acknowledge the problem of prioritisation and its effect on fragmenting EU-level approaches to cyber security, there is no indication provided as to the reasons why some Member States feel some policy areas are more worthy of political attention or resources than others. This highlights a wider problem in academic studies of EU cyber security policy: very often the question *why* something is the case is not asked. This is a gap not only in the specific sense of why Member States prioritise cyber security at a lower level than other areas. Why the EU has adopted a socio-economic approach to cyber security, or why that policy has continued unaltered between 1985 and 2013, are wider questions which have also not been asked.

To date, no academic studies have been conducted which address these wider questions, or which counter the specific position that EU cyber security policy is fragmented. Interviews and primary literature analyses carried out for this thesis indicate the persistence of a division of responsibility for cyber security between the Directorates-General for

Migration and Home Affairs (DG HOME) and Communications Networks, Content & Technology (DG Connect), the External Action Service, and a number of operational agencies involved in the sector, such as the European Network and Information Security Agency (ENISA), Europol and the EU's Computer Emergency Response Team (CERT-EU). The persistence of fragmentation remains a theme in current academic literature on EU cyber security.

This is important because that current academic literature does not address the disconnect between fragmented policy *implementation* and a continuous socio-economic policy *approach*. The fragmented policy environment described by Christou, Klimburg and Tiirmaa-Klaar or Sarma is not one conducive to continuity. With the diverse range of policy areas in which cyber security is relevant and the differing priorities placed upon it by the EU's Member States, a stable policy framework is unlikely to exist, and even less likely to persist. To date, no solutions to this puzzle have been provided.

There is, however, one point of agreement in the corpus of study as to how the EU approaches cyber security more generally. Due to the inherent internationality of cyberspace and its concomitant threats, transnational co-operation is crucial to establishing security in cyberspace. Co-operation as a tool for promoting and even achieving cyber security is a significant feature of the current literature, one which seemingly contradicts the focus on fragmentation. This is of relevance to the thesis's research question because a co-operative environment, or at least an environment where co-operation is encouraged, *is* conducive to policy continuity. This is because co-operation in any policy area requires a certain degree of unity of purpose and shared values between multiple actors, such as the EU's Member States and constituent institutions. The debates in academic literature, however, show that the problem of fragmentation has spilled over into EU efforts to build and facilitate co-operation.

2.2.2. Co-operation as a policy goal

Bendiek and Porter (2013, p. 176) argue that co-operation between the EU, its Member States and private sector entities is vital to tackling a range of cyber security issues. These include illegal content, emergency and crisis response (Bendiek and Porter, 2013, p. 174) and online child sex abuse (Bendiek and Porter, 2013, p. 169). Janczewski and Colarik (2007, p. 13) add that co-operation is crucial even in deterring and tackling information warfare. Cyber warfare is an issue of which the EU must be aware, but which is subject to issues of competence (Robinson, 2012, p. 161). This indicates that the problem of

fragmentation has spilled over into EU solution-building, particularly in its definition of co-operation.

Co-operation as a policy goal is acknowledged in current academic studies. However, it is ill-defined and takes a number of different forms. There is little agreement, consensus or consistency as to what form co-operation should take. Robinson (2014, p. 4) notes that even in the relatively under-developed field of cyber defence, the EU is fostering bilateral arrangements with international partners such as the US, Brazil and China, as well as co-operation with NATO. Christou (2016, p. 105) states that, in the case of cyber-crime, co-operation means bringing together the different interests of stakeholders including judicial authorities and private entities. Cornish (2009, p. 27) notes that co-operation also referred to raising awareness of security issues, something often referred to in primary *acquis* literature. Blythe (2008, p. 89) notes that attempts were also made to enforce co-operation between Member States. As an example he cites *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000* on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. Article 19 of that Directive is dedicated to co-operation. It requires Member States to establish national "contact points". These are to provide communication amongst the Member States and between the Commission on relevant information and changes to national legislative measures which may affect the smooth conduct of electronic commerce (European Parliament & Council of the European Union, 2008). The point made is that co-operation, or at least its facilitation and co-ordination, was a standardised *modus operandi* for the EU in cyber security policy.[5]

Co-operation in EU cyber security therefore takes many different guises. Choucri, Madnick and Ferwerda (2014) provide a *précis* of the problem in their discussion of the institutional foundations of cyber security. They argue that there is an absence of "a co-ordinated industry response to develop collaborative threat reduction strategies". The fragmentation of EU and Member State co-operation stems from a lack of co-ordination in industry. This lack of co-ordination means that co-operation is hindered. What Choucri *et al* do not provide is a resolution to this issue.

As an international organisation the EU has the capacity to provide this co-ordination. Centeno, van Bavel and Burgelman (2005, p. 60) note that, when developing tools for e-

[5] Data analysis undertaken for this thesis provides empirical evidence for this position. See Chapter 5 Section 2.5.

governance[6], the EU was acutely aware of the need for networking, co-ordination, collaboration and better government, as well as "democratic and co-operative policy formulation, citizen and civil society involvement [and] transparent and participative implementation of policies" (Centeno *et al*., 2005, p. 60).

Sliwinski (2014, p. 469) takes this argument further. He argues that the EU not only has the capacity to provide co-ordination, but the tools to do so. Through its specialist agencies, such as the European Network and Information Security Agency (ENISA) and the European Cyber-Crime Centre (EC3), or the Friends of the Presidency on Cyber Issues (Interview, Permanent Representation of Germany to the EU, 2015) the EU as a forum can facilitate this co-operation. There are, however, limits to this facilitative role. As Sliwinski (2014, p. 471) notes, a sector which involves any aspect of foreign and security policy falls under intergovernmental decision-making processes. He argues that this curtails the capacity of the EU to act, given the need for unanimity in the Council of the European Union, "whereby national narratives hamper a truly common vision from emerging" (Sliwinski, 2014, p. 471). In cyber security, co-operation and capacity-building work are crucial in order to enable Member States to move beyond mere co-ordination of efforts in a security field, especially a field with so transnational an outlook, but those efforts may be hampered by Union competences.

This curtailment is predicated upon a view of the EU as a weak or limited actor in cyber security. The argument is made that the EU will not be able to project itself onto the international stage due to "Member States dominating the European action on cyber security challenges over a genuine common response" (Sliwinski, 2014, p. 479). Sliwinski argues that the EU is weak in this regard. However, while the supremacy of Member States in cyber security may well be the case, to describe the EU as a weak actor is perhaps not to do it justice. ENISA is an international advice broker and centre for information-sharing (ENISA, 2005). As Carrapiço and Trauner (2013) note, Europol is an intelligence hub and is ideally placed to influence cyber-crime policy. Sliwinski's position is predicated upon a very narrow definition and conceptualisation of "actor" in this policy area.

Christou and Simpson (2014) counter Sliwinski's pessimistic view of the EU's influence on international cyber security issues. They do this by utilising Bretherton and Vogler's

[6] Such as transparency, access to information and increasing citizen participation in policy development (Centeno et al., 2005, p. 60).

three-part model of "actorness" (Bretherton and Vogler, 2006, pp. 24–30). By having the presence, opportunity, and capability to act in order to shape international norms of Internet governance, the EU is exercising a particular influence as a facilitative international actor, especially when it comes to fostering co-operation. Christou would later equate this facilitative capacity with what makes the EU an actor in international cyber security (Christou, 2016, p. 6). This is a view supported in the wider security context by Zwolski (2013, p. 17) and Rozée (2013, p. 42). As an economic union the aims of the EU are to ensure the safe exploitation of cyberspace for citizens and commercial entities rather than to engage in military or national security actions. To that end Crago (1996, p. 467) argued as early as 1996 that the EU and the Internet have similar goals: "to transcend traditional political, geographical and cultural barriers in order to promote greater regional and transnational co-operation".

This thesis will build on Christou and Simpson's use of Bretherton and Vogler's model. It can be used in a more nuanced fashion when referring to the EU's "actorness". Christou and Simpson use the model to argue that the EU is an actor on the international stage, based on the assumption that its actorness is not yet agreed upon. While this is a valid standpoint, this thesis will take the model one step further. It will accept that the EU is an international actor, and will use Bretherton and Vogler's model to justify this position.

2.2.3. Contribution of this thesis to EU academic literature

The result of this literature review is that there are two areas in which this thesis can make substantive contributions. Although there is a growing body of scholarship studying EU cyber security, only recently has there been a trend towards examining the totality of the policy sector. Scholars such as Christou (2016), Robinson (2012), Sliwinski (2014) and Bendiek (2012) have done so, but such approaches are in the minority. The majority of analyses demonstrate a tendency towards specificity in EU cyber security studies. The development of EU cyber security policy as a sector of Union policy-making has been largely neglected. The scope and rationale for this thesis provides this holistic, whole-of-sector analysis of policy-making processes in order to provide the overarching context and framework which many scholars have argued is missing from EU cyber security itself. This whole-of-sector analysis will help with understanding the continuity of the EU's socio-economic policy approach, and so help to answer the thesis's research question.

Current scholarship also offers very few reasons as to *why* the EU adopted particular policy solutions. This is reflected in those studies which argued that co-operation is the policy of

choice. While acknowledging that co-operation is an important tool, there is little agreement on the nature of that co-operation, and still less discussion of why this choice was made. This highlights the second gap in literature and is symptomatic of a larger omission in EU cyber security scholarship. The EU's policy differs from that of other actors. The prevailing policy narrative is to acknowledge the importance of ICT and cyberspace to national security (Japan, 2013, p. 8; Russian Federation, 2013, pp. 2–3; USA, 2011a, p. 5) and therefore to address cyber security from a defence perspective. A reading of the EUCSS demonstrates that the EU approaches cyber security from a *socio-economic* direction, with no martial language save for a small section on cyber defence that is little more than a passing reference (European Commission, 2013a, p. 11). There is no mention in EU policy of military responses to cyber threats, cyber war or warfare, or the co-ordination of Member States' national security apparatus to combat state-sponsored cyber activity.

Current scholarship has not asked *why* this is the case. Commentators such as Christou, Sliwinski and Centeno *et al* provide insight into *what* the EU is doing to address cyber security challenges, and *how* it goes about this. However, there is little discussion as to the reasons behind the choice of co-operation as a *modus operandi*. This is a significant omission and it is therefore an important aim of this thesis to ask *why* the EU does what it does in cyber security.

Because there have been limited examinations of the background to EU cyber security policy, there is also a lack of in-depth, *theoretically* informed work in this field (Christou, 2016, p. 33). This observation identifies a third area where this thesis can make a contribution. By placing this analysis of cyber security within one of the main theoretical frameworks applied to EU policy-making research, this thesis can provide insight into the EU's policy-making process as a whole.

2.3. Theory

This thesis is an examination of the EU's policy-making mechanisms. To carry out the analysis a suitable theoretical framework will be chosen from amongst those generally employed in analysing EU policy-making. This is important because, in order to undertake an effective social science examination, "researchers need to conduct their inquiries under the auspices of a particular theoretical framework" (Rosamond, 2000, p. 4).

There is a rich heritage of theoretical approaches to the study of the EU. It ranges from gender studies (Locher, 2012) and critical approaches (Cafruny and Ryner, 2003; Manners, 2007) to quantitative assessments of elections and legislative processes (Kovats, 2009). That heritage also went through various phases, where particular approaches were preferred over others (Wiener and Diez, 2009, p. 7). This section of the chapter will examine the applicability to this thesis of four of the most prominent theoretical traditions: neofunctionalism; liberal intergovernmentalism; constructivism and institutionalism.

The research question and ultimate goal of this thesis is to examine the role of institutions and institutional arrangements in the development and continuity of a socio-economic cyber security policy. Despite this premise, the choice of institutionalism as the theoretical framework is not a foregone conclusion. The four approaches examined here have become part of a prevailing narrative for studying European Union policy development (Pollack, 2005, pp. 357–358). They also share an important trait: a focus on teleological processes of social, economic and political integration. Work such as that of Dinan (2010) and Duke (2011) seeks to understand how the concept of "ever closer union" affects the relationships between Member States, the EU's formal institutions, external partners and the Union's policy development architecture. This has affected analyses of fields as diverse as environmental policy (Golub, 1996; Knill and Lenschow, 1998) and the nature of the European welfare state (Taylor-Gooby, 2004).

This poses a problem for conducting holistic examinations of cyber security policy in the EU. The EUCSS – the exemplar of that policy – is not a function of integration. The Union recognises that it is predominantly the task of Member States to "deal with security challenges in cyberspace" (European Commission, 2013a, p. 4). This presents a challenge for positioning this thesis within common theoretical traditions due to their concentration on integration.

This section of the chapter will explore each of these frameworks in turn. Doing this will provide the reasons and justification as to why historical institutionalism (HI) is the most apposite theory for a study of EU cyber security policy-making. The goal is not to reject other frameworks outright. Instead HI will be the *dominant* theoretical approach for this research. Neofunctionalist, intergovernmentalist and constructivist approaches will be used to *inform* the HI analysis. This is particularly the case with constructivism. As will be shown in Chapter 5, the EU has developed – i.e. constructed – an idiosyncratic discourse in cyber security, one representing a departure from the prevailing policy and

academic narrative in that sector. Those narratives tend to focus on pessimistic, fear-laden, and often highly militarised approaches to achieving cyber security. HI can provide a wider theoretical framework than would be possible if utilising constructivist approaches alone. This is because the discourse was developed around certain core path dependencies laid down in the 1980s and 1990s which affected later policy options and choices in the 2000s.

2.3.1. Neofunctionalism

The defining characteristic of neofunctionalism is the effect of functional spill-over on policy choices (Haas, 1958, p. 297). Policy decisions made "pursuant to an initial task and grant of power can be made real only if the task itself is expanded" (Haas, 1961, p. 368). In other words, once a decision is made, there is a tendency for mission-creep to set in, with relevant policy areas being drawn into the purview of the original authority (Cram, 1996, pp. 46–47; Pollack, 2005, p. 359).

This concept appears particularly suited to studies of the EU. Haas (1970, p. 616) argued that the creation of a regional common market, a defining feature of the EU, is the facet most conducive to "rapid regional integration and maximisation of spill-over". Consequently, it is reasonable to assume that the development of the EU's *Cyber Security Strategy* was such a spill-over. The core aim of the EUCSS was to ensure the continued viability and functionality of the Single Market. During the economic recession of the 1980s, European economies were struggling with stagnation and rising unemployment. The institutions of the EU, particularly the Commission, looked for ways and means to break this pattern. The initiation of the Single Market in 1992 was an important part of an overall strategy seeking to capitalise on potential growth sectors. The burgeoning ICT industry was one such sector (European Commission, 1985). Once this precedent had been set – that ICT and the internet would be used for economic growth – infrastructure and citizen security concerns began to be drawn into the nexus of common market sustainability as and when these issues became apparent over the course of the timescape. This can reasonably be assumed to be the result of functional spill-over or unintended and unforeseen consequences of policy decisions (Schmitter, 2004, p. 3). The decisions in question were those regarding the use of information communications technology (ICT) in the internal market as early as 1985 (European Commission, 1985).

An initial examination of pertinent primary literature shows that ICT and the information society were considered crucial to the development and sustainability of the internal

market as far back as 1985 (European Commission, 1985). The relatively simple decision made in that year to pursue the promotion of the ICT industry for wider economic growth necessarily expanded as the sector itself blossomed and citizen and data protection concerns arose through the increased use of Internet-enabled technologies. The ease of access to these new technologies and the amount of private and corporate data being stored on networked systems led to increasing instances of computer-related crime, a concept which would become known as cyber-crime. Similarly, fundamental rights such as citizen privacy and freedom of expression needed to be secured. Not only should every citizen have access to information and digital services, but the platforms that supported them needed to ensure user details were kept private.

Neofunctionalism lends itself as a theoretical framework to a study of EU cyber security policy-making because of the importance of ICT to the continued functioning of the common market. This was particularly relevant in the earliest years of the EU's interest in cyber issues. As will be examined in Chapter 6, the primary purpose of the EU's interest in the nascent IT sector was its potential to galvanise economic growth and fuel employment (European Commission, 1985, 1994, 1996b). The prioritisation placed on economic maximisation endured throughout the entire policy-making timescape from 1985 to 2013. A core tenet of the 2013 *Cyber Security Strategy of the EU* – the culmination of the cyber policy-making process – is the protection and safety of key ICT infrastructures underpinning the Digital Single Market, itself a vital piece of the wider Single Market project (European Commission, 2013a, p. 2). Although not following a teleological, deterministic path, cyber security and the EU's approach to that field can be seen as a spill-over of the drive to create, develop and maintain the internal market.

However, deeper examination of both cyber security and neofunctionalism demonstrates that the two are not as compatible as may at first appear. There are two problems with applying neofunctionalism to cyber security. The first is a question of competences. Cyber security occupies a grey area between economic policy, where the Union has extensive competences, and national security considerations, where EU action is severely restricted. The second problem is EU cyber security not being a function of integration.

2.3.1.1. Neofunctionalism, Cyber Security and Limited EU competences in defence policy

Consider the following hypothetical scenario: the nationalised bank of an EU Member State experiences a distributed denial of service (DDoS) attack which paralyses its online

banking systems, preventing account holders from carrying out transactions. This type of cyber-incident is an economic, criminal act. But if the cascading consequences of that incident were to affect the entire banking sector and financial infrastructure of the Member State, then it can become a national security concern. The incident can potentially affect state stability internally or even internationally. The issue is further complicated by the fact that the precise technical manoeuvres and actions undertaken in a cyber incident are the same whatever the target and whomever the perpetrator. What differentiates one cyber incident from another are the intentions of the perpetrator, who often hides behind the anonymising capacities of cyberspace. This is known as the "attribution problem" (Dunn Cavelty, 2012a, p. 12; Gaycken, 2011, p. 80; Tsagourias, 2012).

The issue facing the use of neofunctionalism in this hypothetical scenario, and in this thesis, is one of Union competences. Due to being both an economic and security concern, cyber security is subject to a continual battle of wills between EU functionaries managing the Single Market and the security concerns of individual Member States. There is a connection between the internal market and the socio-economic consequences of insecure ICT infrastructures (Interview, Smith and Jones, eu-LISA, 2014). Large, pan-European networks such as the Schengen management system and the asylum-seeker database are areas where the EU has higher levels of competence. However, there is a potential for large-scale, cascading cyber incidents to affect critical *national* infrastructures. This means nation states, including the Member States of the EU, consider cyber security policy alongside, and sometimes within, national security concerns (Estonia, 2008; UK, 2011).

Following the entry into force of the Single European Act in 1987, the EU is restricted to political and economic aspects of security. EU Member States are cautious about transferring too much power from national governments to the EU in security matters. The EU therefore has very specific rules regarding the extent to which it can become involved in a policy area considered a national security issue. This restriction necessarily colours the manner in which the EU approaches security risks emanating from cyberspace[7]. As exemplified in the scaling back of efforts to prescribe specific solutions following the failure of the Constitutional Treaty in 2005, Member States slowed down integrationist aspects in cyber security, despite that policy area's relevance to the Digital Single Market. They wanted the EU to operate within the strictest interpretation of its remit in the Treaties (Interview, Senior Official, BIS UK, 2014). This meant a functional spill-over could not

[7] This interpretation is examined in greater detail in Chapter 8.

occur in cyber security policy as restrictions on EU action were tightening. This prevention of spill-over - a core tenet of neofunctionalism – calls into question the applicability of neofunctionalism to this thesis.

2.3.1.2. Neofunctionalism, Cyber Security and a Lack of Integration

This applicability is dealt a further blow by the fact that, as argued by Christou (2016) and as stated in the EUCSS itself (European Commission, 2013a, p. 4), the EU is explicit in the view that responding to security challenges in cyberspace remains the responsibility of the Member States rather than any supranational body. While a number of important initiatives were undertaken in the field of criminal justice (European Parliament & Council of The European Union, 2002, 2011), and the EC3 is making strong headway in tackling computer-related crime (Mendez, 2005, pp. 518–519), Europol itself has no executive powers. It cannot make arrests on behalf of the EU or its Member States[8] (Interview, Senior Official, Europol, 2014). Similarly, ENISA, a crucial part of the EU's approach to cyber security, does not provide security. Instead it acts as an information hub (Sliwinski, 2014, p. 477). It is an advice broker, assisting those entities, public and private, who actually do the securing.

Cyber security is not a policy sector which promotes integration. Although it does not explicitly disavow any connection to the concept of ever closer union, the EUCSS acknowledges that the tools and responsibility for achieving cyber security are in the hands of the Member States. Cyber security cannot, therefore, reasonably be considered a result of functional spill-over from increasing political and policy integration. This ultimately makes neofunctionalism a less than ideal theoretical framework for this study.

2.3.2. Intergovernmentalism

According to Pollack (2005, p. 360), intergovernmentalism developed out of a concern that neofunctionalist research focussed on supranational entities at the expense of the nation state. A more fruitful manner in which to examine the EU was to concentrate on the interaction of sovereign entities – i.e. intergovernmental interaction. The reaction to supranationalism began with Hoffman (1966). Instead of nation states – in this context the Member States of the EU – being obsolete given the rise in prevalence and power of supranational entities like the EU, their primacy *within* these international architectures was proving surprisingly resilient. This resilience is predicated upon the legitimacy of

[8] It is perhaps pertinent to acknowledge, however, that this issue is not unique to cyber-crime. Europol has no executive powers in any field.

national self-determination – the sovereignty of the nation state – and what Hoffman called the

> newness of many of the states, which have wrested their independence by a nationalist upsurge and are unlikely to throw or give away what they have obtained only too recently (Hoffmann, 1966, p. 864)[9].

The concept of the primacy of the nation state within or in spite of any supranational entity is particularly relevant to a discussion of the EU and the development of Union policies, particularly cyber security. As demonstrated by Sliwinski (2014), the EU has no executive powers in core areas of cyber security such as computer-related crime. Similarly, cyber security is often considered a national security issue. Member States are at best reluctant to delegate power in this area upwards to any supranational body, institution or agency. The EUCSS also explicitly acknowledges Member State primacy in this field.

There are two reasons for this restriction. On the one hand there is the explicit purpose of the EU as an economic rather than security entity. The EU started life as a pooling of the coal and steel industries of six countries (Dinan, 2010, p. 17). On the other hand was the codification of the EU's position on security policy in the 1987 Single European Act and the 1992 Petersburg Tasks (see Chapter 6 Section 3.1). These restricted the EU's involvement to the "political and economic aspects of security" (European Union, 1987, p. 1049). The important point, according to Pollack, is that neofunctionalism had "underestimated the resilience of the nation-state" (Pollack, 2005, p. 360), an underestimation which intergovernmentalism could redress.

Building on this notion of the primacy of the nation state within a political organisation, Moravcsik (1993, pp. 484–487) developed a three-step model for intergovernmental European integration. This model moved away from the idea that the supranational entity drives the process, and is predicated upon states as rational actors bringing their preferences to a bargaining forum. At the first level, the national governments aggregate the preferences of their constituents into recognisable and (ideally) agreed policies which represent the interests and goals of those nation states. These goals are brought to the second level of the model, the intergovernmental bargaining table in Brussels. National governments engage in "hardball bargaining" (Pollack, 2005, p. 361) amongst their fellow Member States in an interest-maximising mechanism. Only once some sort of agreement

[9] This is a reference to the period of post-war nationalism which saw an increasing number of European colonial territories declaring or being granted independence.

is made do the Member States elect to pool sovereignty in supranational institutions in order to ensure collective compliance and to

> overcome the almost inevitable interstate prisoner's dilemma of enforcement, whereby individual governments seek to evade inconvenient responsibilities, thereby undermining the integrity of the entire system (Moravcsik, 1993, p. 512).

In effect, the supranational entity is relegated to a body whose sole purpose is to ensure that its members comply with certain rules and obligations.

The intergovernmentalist model would appear to suit a study of cyber security policy because that sector contains explicit acknowledgment that the Member States retain ultimate responsibility for ensuring and providing such security (European Commission, 2013a, p. 4). Bendiek's (2012, p. 19) analysis acknowledges the Union's role in facilitating co-ordination and co-operation between the responsible cyber security actors. This explicit acknowledgment would appear to give intergovernmentalism the upper hand as a theoretical approach for this thesis.

The drawback for such a study of EU cyber security, however, is that there is no pooling of sovereignty in this particular policy area. This omits a vital component of Moravcsik's model. As mentioned above, the EUCSS clarifies that Member States retain responsibility, i.e. they retain sovereignty, in securing national digital infrastructures. Agencies such as ENISA and the EC3 operate as information hubs. Member State sovereignty or authority is not pooled in this policy area.

While liberal intergovernmentalism and Moravcsik's three-level model for policy analysis may appear to be suited to a study of this nature they are rendered *unsuitable* due to the EU's Member States reluctance to delegate cyber security matters upwards to EU level. The Member States have chosen *not to* give the EU competence to act. As Craig (2010, p. 182) argues, even after the entry into force of the Treaty of Lisbon, the area of the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP) remain sectors of unanimous Council decision-making, and are not subject to the qualified majority voting processes. They are considered sections of "special competence" (European Union, n.d.). As a result Member States are reluctant to and even refuse to pool resources, let alone sovereignty, in a field so intimately connected to national infrastructure protection and defence. In addition, in the EU policy-making infrastructure, cyber security is not wholly positioned within any of the policy areas subject to intergovernmental decision-making.

Cyber security is therefore a paradox for the EU which weakens the applicability of Moravcsik's intergovernmentalist mode of EU study. The Union places a socio-economic interpretation on the nature of cyber-risks. These are considered issues which threaten citizen wellbeing and the functionality of the internal market. This in turn means that core aspects of cyber security fall under the aegis of Home Affairs and the Single Market. Both of these areas fall under the supranational, qualified majority voting mechanisms, rather than the unanimous intergovernmental processes of defence and security. However, cyber security is both a hard security matter when defence policy is being discussed, but also a socio-economic, criminal justice matter when the internal market is on the agenda. This provides an opportunity for researchers to examine a policy area which contains the best, or worst, of both supranational and intergovernmental worlds. For the purposes of this thesis, however, this paradox means that intergovernmentalism is not the most suitable framework for analysis.

2.3.3. Constructivism

Constructivism also appears, at first glance, to be eminently suited to a study of the development of EU cyber security policy. The core premise of constructivism is the existence of a "social process though which agent [i.e. actor] properties and preferences change as a result of interaction" (Checkel and Moravcsik, 2001, p. 220). Policy choices are made as a result of this social process.

The general academic and policy discourses on cyber security, beyond the immediate confines of the EU, contain a number of core themes. These range from technical discussions regarding the vulnerabilities and security measures required for supervisory control and data acquisition (SCADA) systems (Morris et al., 2011; Simões et al., 2015) to the relative advantages of honey-pots over hack-back in conducting active cyber defence (Lachow, 2013; Dewar, 2014, p. 13). Decisions regarding cyber security policy are made based on an interpretation of those discourses. A privately-owned technology company will have different cyber security priorities to a state-owned energy concern or a heavily connected nation-state such as Estonia. Similarly, the EU's interpretation of these general cyber security discourses is predicated upon it being a socio-economic entity. This makes it more of a target for corporate espionage and computer-based crime than state-sponsored cyber warfare[10]. The decisions made by the EU's constituent actors – its formal

[10] Notwithstanding the 2007 DDoS incident in Estonia, alleging Russian involvement.

institutions and the Member States – are therefore informed by the Union's own *internal* cyber security discourse.

This has led to a particular EU *interpretation* of the nature of security threats and risks emanating from cyberspace. Even those risks which infer state-sponsored activity bordering on acts of war are interpreted by the EU as threats to several *socio-economic* concerns. These include the ongoing functionality of the Single Market, personal and data privacy, and taking advantage of the opportunities afforded by universal access to the latest in digital technology. In short, these threats are subject to a socio-economic construction which has developed over time.

As with neofunctionalism and liberal intergovernmentalism, constructivism appears on the surface to be a theoretical framework which would provide some insight into why the EU does what it does in the field of cyber security. The EU's cyber security policy and strategy, set out in the 2013 EUCSS, is an interpretation or construction of those aspects of a general cyber security discourse which are (a) most relevant to the EU and (b) most suited to the EU's core socio-economic competences. The Union is seeking to secure cyberspace to ensure the security and viability of the common market. It therefore focusses on reducing and tackling those risks, such as computer-related crime and attacks on privacy, which may have a negative effect on that market.

While constructivism as a theoretical approach may appear entirely appropriate for this thesis, there are two aspects of the theory which raise red flags. First, constructivism is often pitched at the level of theory or metatheory (Checkel and Moravcsik, 2001, p. 219). Even self-confessed constructivist research such as Koslowski's (1999) examination of the quasi-federal nature of Member State bargaining, or Hyde-Price and Jeffery's (2001) research into the influence of Germany in the EU, assume a macro-theoretical position focussing on very broad themes. While this thesis examines a long period of time (28 years between 1985 and 2013), conducting macro-theoretic examinations is not the aim of this research. Rather, the aim is to examine the single policy area of cyber security over that specified period of time. This makes constructivism arguably too broad a mechanism. While it is indeed the case that the EU's narrative in the field is constructed, and that construction is influenced by actor and institutional decisions (Wendt, 1995, p. 303), constructivist approaches such as those of Wendt or Checkel (1999) are perhaps better suited to examining large, substantive issues such as the totality of the cyber security

narrative – civilian, military, criminal, technical, European, American etc. – or the large-sale problem of European integration.

The particular reason that constructivism is not best suited to this study is the overall aim of the thesis. This research seeks to contribute to academic understanding of the EU. It will do this by studying the institutions, institutional arrangements, social processes and drivers which have led to the EU developing its approach to cyber security. This is a constructivist approach. However, the thesis also seeks to understand the causal mechanisms which have led the EU to adopt and maintain a position at variance with the prevailing cyber security narrative. Checkel and Moravcsik (2001, p. 221) argue that causal mechanisms underlying social processes are often neglected in constructivist analyses. Such analyses rarely account for any variation in international norms (Sikkink and Risse, 1999, p. 4). It is precisely this variation or divergence which this thesis seeks to understand. This makes constructivism less applicable than it at first appears.

This research does not reject constructivism as a theoretical framework outright, however. Instead, constructivism will be employed to supplement and inform the framework which will be employed: historical institutionalism. Analysing the causal mechanisms of a particular interpretation of policy *over time* will facilitate the examination, and develop the understanding of, the EU's approach to cyber security.

2.3.4. Institutionalism

The final branch of theory most pertinent and appropriate to this thesis is institutionalism. This approach is predicated upon studying the influence of institutional forces on social, economic and political phenomena. To bring clarity to this position, Hall and Taylor (1996) establish three "types" of institutional analysis: rational choice institutionalism, historical institutionalism and sociological institutionalism. While not going so far as to claim separate methodologies for the three types, Hall and Taylor argue that these were in fact three different *approaches* to the study of the role of institutional drivers of change and actor preference (Hall & Taylor, 1996; Steinmo, 2008, p. 118; Bache, George, & Bulmer, 2011). Although distinct, the three approaches are mutually complementary and share the same key trait: examining the influence of institutions on the interaction of rational actors. Where they differ is in the priorities they place on key features of that interaction, the preferences actors bring to it, and perhaps most crucially, on the precise nature of institutions.

Rational choice institutionalism (RCI) is predicated upon understanding actor preference within an institutional setting. Steinmo (2008, p. 162) argues that, in RCI, institutions frame individual actor behaviour and preferences. These preferences are exogenous: they are brought to the formal arena of interaction and are limited by it (Hall & Taylor, 1996, p. 943). The goals and values of the institution restrict the actors' capacity to achieve all of their aims in what is known as "bounded rationality" (Peters, 2005, p. 56). Nevertheless, there is a certain utility to engaging with an institution and the actors within it: the reason actors choose to co-operate is because they get more with co-operation than without it (Steinmo, 2008, p. 127).

Sociological institutionalism (SI) by contrast focusses less on the formal structures of the arena of interaction, and describes as institutions anything that "provides [a] frame of meaning guiding human action" (Bache et al., 2011, p. 26). Accordingly, cultural constructs such as religions, ideologies, social class or any collection of "culturally specific properties" (Hall and Taylor, 1996, p. 946) are also institutional constructions and influence policy decisions. SI therefore blurs the lines between formal institutions and abstract culture, enabling a more nuanced study of political processes. Furthermore, it stipulates that institutions affect not only the calculations made by individuals in political interaction, but also their most basic preferences and even their identity (Hall & Taylor, 1996, p. 947) prior to their engagement with the institution.

Finally, historical institutionalist (HI)[11] scholarship argues that key decisions made at the inception or initiation of an institutional body continue to influence the subsequent evolution of the institution and determine the tenor of future policy decisions made by actors (Peters, 2005, p. 71). Rather than treat institutions as arena structures where the political interaction is the most significant element, HI represents an attempt to show how political struggles are "mediated by the institutional forces in which they take place" (Thelen and Steinmo, 1992, p. 2).

The key aspect which differentiates HI from rational and sociological variants is that an HI framework "recognises that political development must be understood as a process that unfolds over time" (Pierson, 2000, p. 264). As shown in Chapters 1 and 3, this notion of temporal longevity is key to the structure and research framework of this thesis. Policies, political action, social strategies and solution-building may occur on an *ad hoc* basis in

[11] The coining of the term "historical Institutionalism" is attributed to Thelen and Steinmo (1992, p. 1) in the first chapter of their volume *Structuring Politics: Historical Institutionalism in Comparative Analysis*.

response to particular exogenous shocks. However, the tenor and nuances of the policy solutions adopted are based on norms and paths set down much earlier in the policy process, even at the establishment of the institutions in which they are developed. This leads to the concept of a "timescape": the temporal features of decision-making that exist across the polity, politics and policy dimensions (Bulmer, 2009, p. 307; Meyer-Sahling and Goetz, 2009, pp. 326–327). Future policy decisions and actor preferences will be directly affected by, for example, the values and goals of the institutions set down at their foundation. In the case of the EU, the establishment of a socio-economic cyber security discourse makes such solutions more likely to be selected over other, more militaristic, national security-focused measures. This is an effect known as "path dependency" (Pierson, 2000; Thelen and Steinmo, 1992, p. 2).

Path dependency functions in a similar way to Haas's process of functional spill-over (Haas, 1961, p. 368). Certain policies and modes of actor behaviour endure over time due to the difficulty involved in unseating long-standing attitudes and policies. Where path dependency differs from spill-over is that the initial task or decision is not expanded to incorporate functionally or ideologically similar areas. Instead, subsequent tasks and policy choices are dependent on the initial decision. Krasner (1984, p. 240) explains that when a policy is embarked upon, the institution enters a period of stasis, continuing on its path until an event or critical juncture shifts the policy into a new period of stasis: so called "punctuated equilibrium". The punctuation point could be an external catalytic event generating particular policy decisions which deviate from the original equilibrium. In cyber security analyses, examples of such catalytic events include the 2007 cyber-attacks on the Estonian banking sector or the 2014 Snowden revelations. Chapters 8 and 9 examine a series of major events which occurred between 2007 and 2009 and which severely tested the strength of path dependent forces in EU cyber security.

In addition to path dependency, another key feature of HI is that actor preferences and decisions must be contextualised, and that context studied *over a period of time*. It is not enough to examine the immediate causes of a policy decision *in situ*. The full background of that decision must be understood. Such historical study of political interaction lends a certain empirical basis to institutionalism (Pierson and Skocpol, 2002, p. 2). What HI does is provide a durational context for political and social interaction which goes beyond the immediate cause of political decisions (Thelen, 2002, p. 93). Such a provision means that HI lends itself to the study of the European Union and EU policy-making in general – and this study of cyber security policy more specifically – as it enables a more nuanced study

beyond simple interest-based, cause-and-effect decision-making explanations. The institutional structure of the EU affects the decisions taken by the constituent actors involved in those institutions but that interaction takes place within the overarching political landscape established by the Union's operational treaties.

In summary, HI as an approach to the study of politics

> pays attention to real world empirical questions, its historical orientation and its attention to the ways in which institutions structure and shape political behaviour and outcomes (Steinmo, 2008, p. 118).

HI scholars are sceptical when seeking to establish large universal laws for actor behaviour. Instead they focus on contextualised theory-building to develop deeper understandings of causal relationships through "an intense and focused examination of…carefully selected cases" (Thelen, 2002, p. 95). For the study of cyber security, HI adds a long-term, longitudinal component missing from much of the current discourse in the field and other theoretical approaches.

Bannerman and Haggart (2014, p. 1) support the point that historical institutionalism is one of the dominant approaches in studies of the European Union. The topics analysed under its banner range from abstract, macro-level examinations of the logic of integration and decision-making (Kerremans, 1996; Pierson, 1996), through meso-level investigations of the governance of the single market (Bulmer, 1998) to analyses of specific policy fields such as telecommunications (Goodman, 2006) or the development of economic and monetary union (Verdun, 2015, 2007). Jupille and Caporaso's (1999, p. 430) review of institutionalist literature and theory as applied to the EU concluded that the "institutional turn" of the late 1990s provided an ability to generalize about EU actor-institution relationships. This placed EU studies more centrally within the broader HI theory literature itself (Jupille and Caporaso, 1999, p. 441). HI is therefore an eminently suitable theoretical framework for examining EU policy development in general, and cyber security policy more specifically.

One final consideration brought to the fore by the range of issues to which HI analysis has been applied, and which highlights HI's appropriateness to this thesis, is that it is not so heavily focussed on integration. Studies of the EU which employ HI, such as the work of Pierson (1996), Bulmer (2008; Bulmer and Padgett, 2005) or Hall (1998) acknowledge the importance of integration. Mühlböck and Rittberger (2015, p. 11) argue that HI has been prominently applied to this topic, in particular to studies of the Council of the European

Union and the Parliament. Integration is not however, the sole focus. As a result, HI is, as Bulmer (1997, p. 368) states, "agnostic on the end-goal of the integration process". This agnosticism fits with the implicit denial of integration in the EUCSS itself. The main concern with employing neofunctionalism, intergovernmentalism or constructivism as theoretical frameworks for this research is those theories' concentration on integration. Cyber security is not an integrationist policy in the EU. A theoretical framework which does not place so heavy a concentration on this aspect of EU policy, such as HI, is therefore more appropriate. The precise mechanisms of HI as an approach to the study of EU policy-making processes and phenomena will be set out in Chapter 4.

2.4. Conclusion

This chapter has shown that there are a number of academic debates and discussions relating to EU cyber security policy. Current research examines the Union's capacity to respond to online criminal activity, evaluations of the relations between important international intelligence actors, the long-term influence of the EU as a protector of fundamental rights and examinations of the influence of Union policy on the technology industry. An important element running through these discussions is the capacity of the EU to facilitate the development of security by ensuring that responsible actors co-operate with one another, rather than provide security itself. As an international organisation made up of independent Member States, the EU is ideally placed to be such a facilitative actor (Crago, 1996, p. 469).

From a cyber security policy perspective, however, there is a recognition that the EU's overall approach has been fragmented. While this highlights an important aspect of EU policy in this sector, it also highlights two gaps in current scholarship. Research undertaken to date does not take account of steps the EU has taken to address this fragmentation. Although these measures were not successful until 2013, there were a series of attempts between 1985 and 2013 to create a general cyber security policy. These attempts are not given full consideration in the literature. The second gap concerns why this fragmentation occurred. One reason for this is that EU Member States place different priorities on cyber security policy. While the existence of this variance is acknowledged in the literature, it is an afterthought in a number of analyses. This misses an opportunity to ask *why* EU policy is fragmented.

The literature review also highlighted a lack of academic attention given to EU cyber security as a policy sector in its own right. While there are recent moves to address this

imbalance, this is still a developing field. This thesis is therefore positioned to make a substantive contribution to EU academic research by conducting a holistic study of the *development* of policy in that whole sector. Current studies have focussed on the operationalisation of policy – *how* the EU achieves cyber security – while little attention has been paid to *why*. This thesis seeks to address this gap in the literature.

The chapter also identified a dearth of theoretically focussed research addressing EU cyber security. This means that identifying theoretical approaches *suitable* to cyber security is problematic. The most commonly applied approaches of neofunctionalism, intergovernmentalism and constructivism each have particular drawbacks when being considered for a study of EU cyber security policy. The most significant of these is a heavy focus on integration. Because the EU recognises that cyber security is predominantly the responsibility of the Member States, an approach concentrating on integration is not entirely appropriate. The chapter has shown that historical institutionalism, also a frequently applied approach to studies of the EU, is more suitable for two reasons. First, it eschews a concentration on integration, and second, it is suited to a long term, temporal analysis. Cyber security policy has been a part of EU policy-making for a longer time than is acknowledged in the literature. The thesis can therefore make a second contribution to academic studies of the EU by conducting an HI analysis in a policy area where such studies have not been carried out.

Chapter 3 | Research Design, Methodology and Ethics

3.1. Introduction

This chapter sets out the methodological process by which the research was carried out. Two distinct source types were used to gather data for the research. Union *acquis communautaire* was analysed in order to identify the EU's cyber security policy itself. However, these documents represent the end-point of a process of development. They provide little indication of influences and drivers in that process. Elite interviews with relevant functionaries directly involved in the policy development process were undertaken in order to provide this insight.

To carry out an effective analysis, the thesis adopted a mixed-methods approach. In the first instance, a quantitative approach was used to identify the institutional and non-institutional drivers pertinent to cyber security policy. Such a technique was necessary because there are a large number of institutional forces involved in developing policy in the EU. There are a similarly large number of entities and bodies involved in that process. Not all institutions and actors are relevant to cyber security. A quantitative exercise was required to draw out those of relevance.

This exercise encountered a methodological problem: interviews and literature sources are subject to differing tools for data extraction. To mitigate this issue, a conceptual content analysis was developed. This involved counting the occurrence of synonymous concepts rather than individual words. The development of this conceptual content analysis enabled the use of a single technique to code and gather data from both literature and interview sources. A model was developed which utilised conceptual, qualitative data combined with a quantitative HI analysis. This model demonstrates how the gap between qualitative and quantitative data can be effectively bridged given the interaction between the two kinds of data (Tarrow, 2010, p. 102).

Having established the pertinent institutions, actors and non-institutional elements, it was necessary to analyse their interaction to understand their role in cyber security policy development. To do this, a qualitative analysis was conducted. A narrative inquiry was carried out in order to study policy development over time and identify the causal chain and mechanisms (George and Bennett, 2005, p. 206) which led to the development of the EUCSS in 2013. This examination of the interplay of institutional and non-institutional

elements over time adheres to Skocpol and Pierson's mechanisms of an historical institutionalist (HI) analysis (Pierson and Skocpol, 2002, p. 3).

The research process was greatly assisted by the use of NVivo software. NVivo is one of a number of computer-assisted qualitative data analysis (CAQDAS) packages available to researchers (Bryman, 2008, p. 565). Operating on a code-and-retrieve theme, NVivo facilitates the examination and coding of text, significantly reducing the labour involved when working with hard copies. In that sense, this programme, and others that carry out CAQDAS are tools to *facilitate* the handling, management and analysis of large quantities of text. As Sprokkereef (in Bryman, 2008, p. 566) notes, what these possible software solutions do not provide are decisions regarding the coding and analysis of the data extracted. Such decisions must be made by the researcher.

This chapter is divided into five sections. Following this introduction, the second section examines how data sources were identified and selected. The third section sets out the conceptual content analysis techniques undertaken to identify the institutions and actors to be examined in this study. It also sets out the methodology undertaken to effectively code the data sources. The fourth section of the chapter explains the narrative inquiry undertaken to examine the interaction of institutional and non-institutional drivers over time. This section explores the qualitative aspect of the research methodology. A fifth and final section provides some reflections on the strengths and weaknesses of the methods used in this thesis.

3.2. Identifying Data Sources

Two source types were used to generate data for this thesis: primary literature and elite interviews. Primary literature included press releases and speeches. However, the most relevant literature was derived from the EU's *acquis communautaire*. As stated in Chapter 1, Union *acquis* comprises

- "the content, principles and political objectives of the Treaties;
- legislation adopted pursuant to the Treaties and the case law of the Court of Justice;
- declarations and resolutions adopted by the Union;
- instruments under the Common Foreign and Security Policy;
- international agreements concluded by the Union and those entered into by the Member States among themselves within the sphere of the Union's activities" (European Union, n.d.)

For the purposes of this thesis, the term *acquis* will also be used to refer to Commission Communications as well as resolutions and conclusions of both the Council of the

European Union and the European Council. This can be justified because these documents fall under the definition of "declarations and resolutions adopted by the Union" cited above.

This thesis used *acquis* as a data source because it comprises the Union's policy in any sector in its purview. Any research examining what influenced choices in the policy development process must include an examination of relevant *acquis*.

3.2.1. Identifying, collecting, collating and cataloguing primary literature

Before any analysis could begin, it was necessary to identify and catalogue *acquis* documents relevant to cyber security. The process of selecting literature sources was facilitated by three specific tools. The first of these was a list of documents relevant to network and information security (NIS) provided upon email request by the European Commission's Directorate General for Communications Networks, Content & Technology (DG Connect) (European Commission, 2012a). This list was provided for previous postgraduate research (Dewar, 2012) and established a starting point for compiling relevant *acquis*[12].

The documents listed cross-referenced each other. For example, *COM (2006) 251 A Strategy for a Secure Information Society* made direct reference to *COM (2001) 298 Network and Information Security: Proposal for A European Policy Approach* (European Commission, 2006a, p. 3). This confirmed both documents' relevance to this study. The earliest listed document, the 2001 *Proposal for a European Policy Approach* (European Commission, 2001a), referred to earlier publications not on the DG Connect list. This inferred the existence of a chronology or policy timescape going back to a point earlier than the list itself provided. This in turn implied that the bibliography of relevant *acquis communautaire* was incomplete and could be expanded.

Having established a core list of relevant documentation, further *acquis* was searched for and identified using two additional tools. The first of these is the official online repository of EU legislation and documentation, the EUR-Lex: Access to European Union Law database[13]. The second was another online resource, the University of Pittsburgh's Archive of European Integration (AEI)[14]. Both of these resources provide online access to

[12] The list itself is provided in full at Appendix 1.
[13] Accessible at http://eur-lex.europa.eu/homepage.html
[14] Accessible at http://aei.pitt.edu/

EU documents in the public domain. This includes Commission Communications such as legislative white papers, and specific legislative instruments such as Regulations, Decisions and Directives. Where documents already identified as relevant to this thesis made reference to specific instruments or publications, these were searched for first in the EUR-Lex database. When not accessible via EUR-Lex, the AEI database was used.

Searching these online databases raised challenges from the commencement of the source collection processes. It was difficult to reliably and efficiently distinguish *acquis* relevant to this thesis from the tens of thousands of documents published by the EU across the full range of its policy areas. When an *acquis* instrument of potential relevance was identified a test was required to confirm whether or not it was pertinent to this study.

A hoop test (Bennett & Checkel, 2015, pp. 17–18; Bennett, 2010, p. 210) was devised to determine the relevance of *acquis* documents. A standard metric content analysis was carried out on the EUCSS itself and the documents in the DG Connect list. This identified eight keywords and phrases frequently occurring in all the documents. Due to differences in the spelling of "online" and "on-line", this equated to nine discrete search terms. These search terms were:

1. Cyber
2. Information
3. Network
4. Digital
5. Internet
6. Communication
7. Online
8. On-line
9. Electronic

When a document was identified as potentially relevant, these keywords and phrases provided a schedule of terms which were searched for to confirm this. Where they occurred the documents were categorised as relevant and catalogued in an Excel spreadsheet. An additional benefit for employing this keyword hoop-test was the fact that, other than Commission Communications, few EU documents were published with sector specific titles. European Council and Council of the European Union's Resolutions use meeting dates or committee names for referencing, because the topics "information technology" or "online communications" comprise two of several different policy areas discussed at those meetings. Commission Communications by contrast are sector and issue specific, and so use discrete titles. By repeating this process of document cross-

referencing, referral and hoop testing a library of 143 relevant pieces of *acquis* was compiled. This primary literature comprised legislative instruments, Council Resolutions and Conclusions, Treaties and Commission Communications[15].

Within the Excel spreadsheet the complete library of *acquis* was categorised by publishing actor or legislative instrument, and then placed in chronological order[16]. This immediately yielded two significant findings: first, that the Commission was the actor most involved with policy-making in cyber security. Of the 143 documents published, including legislation and treaties, 48, or 33.5%, were published by the Commission alone. While this was to be expected considering the Commission's role as a policy initiator, this finding did not confirm whether or not the Commission was the most *powerful* actor in this sector. Instead it signified that it was the most *involved* actor, and established the Commission as an important target when seeking participants for interview.

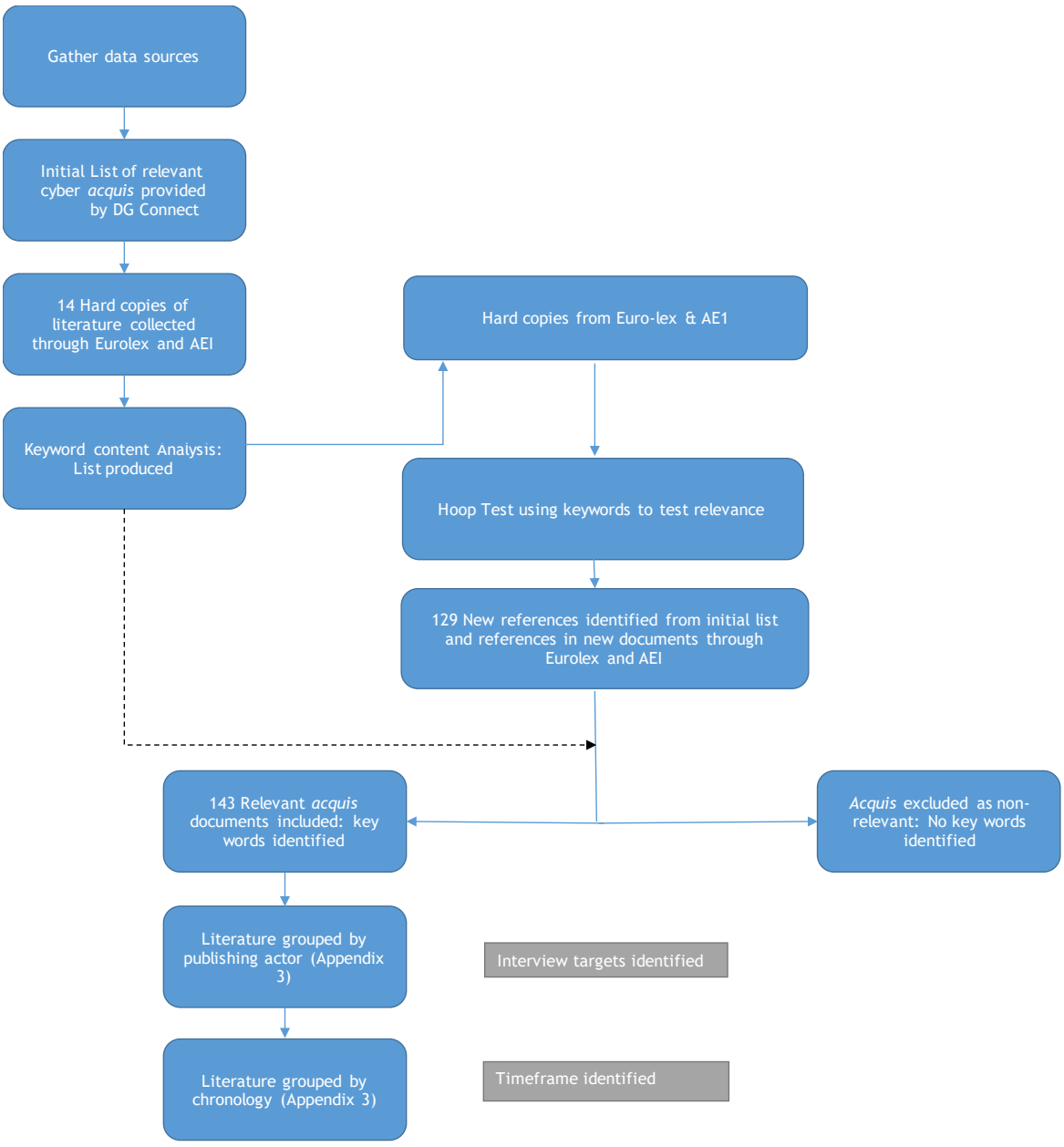
Arranging the *acquis* in chronological order also provided a full timescape for the research: the period between 1985 and 2013. This was a period of 28 years beginning with the Commission's plans to initiate a single market between the Member States, and culminating in the publication of the EUCSS itself, the end product of the cyber security policy-making process.

Finally, the chronology identified a series of milestones in the development of cyber security policy. Key documents were published in 1985, 1994, 1996, 2001, 2006 and 2013 which bookmarked specific periods of ideational development. These documents would be the foci for examining the timescape, the final stage in the research. To effect and facilitate that analysis, all the primary literature documents were uploaded into NVivo computer-assisted qualitative data analysis software (CAQDAS).

The *acquis* collection process is illustrated in Diagram 3-1 below.

[15] The spreadsheet containing the complete of *acquis communautaire* is provided in Appendix 2.
[16] See Appendix 3 for the spreadsheet of *acquis* arranged chronologically by publishing actor.

Diagram 3-1: *Acquis* collection process



3.2.2. Elite interviews

The second source of data was a series of elite interviews, of which 29 were referable. Elite interviewing was chosen as a data collection tool because primary literature could provide only one part of an analysis of policy-making processes. The EU's *acquis* by its very nature represents the end point of development. It is a finished product which provides few insights into its developmental or generative processes. Interviews with functionaries who *wrote* the *acquis* can provide experiential insights, motivations and indications of specific drivers not immediately obvious or clear from policy documents. Elite interviews therefore complete the analysis.

3.2.2.1. Selection/identification of Participants

There were two types of interview participants. The first type comprised relevant officials and bureaucrats. This included functionaries of the EU's formal institutions and its agencies as well as current Member State civil servants working within the field of cyber security. This included representatives from Europol, the European Network and Information Security Agency (ENISA), relevant Directorates-General at the European Commission, Members of and functionaries from the European Parliament, and national government representatives. The second type of participant comprised academics and researchers at universities and private research agencies with specialisms in European or general cyber security. Participation was secured with representatives from agencies including the International Centre for Defence and Security (ICDS) in Tallinn, the Security and Defence Agency (SDA) in Brussels and Chatham House in London.

The selection of primary literature sources outlined in Section 3.2.1 above enabled the identification of organisations and agencies closely involved with cyber security in the European Union. The categorisation of *acquis communautaire* by publishing actor and by document type identified the European Commission, the Council of the European Union and the European Council as important actors, which in turn established these as "targets" for interview participants. Of particular note at this juncture is the fact that the European Parliament was not identified in the *acquis* collection exercise as an actor involved in policy development. Nevertheless, functionaries and MEPs from the European Parliament were targeted for participation in the research to establish if this was a trend or an aberration in the *acquis*.

The *acquis* collection exercise also highlighted subsections within actors where participants should be sought. This was particularly prevalent in the European Commission. The collegiate nature of that actor meant that several departments within it – known as Directorates-General (DGs) – were involved in the development of cyber security policy. An investigation into the *acquis*, commencing with the EUCSS itself, was able to highlight those DGs most relevant to this research. These were the Directorate-General for Migration and Home Affairs (DG HOME) and the Directorate-General for Communications Networks, Content & Technology (DG Connect). The EUCSS also demonstrated that the European External Action Service (EEAS) was a core member of the group developing that strategy. Interviews were sought at these three bodies in the first instance.

Because the *acquis* only referenced actors or actors' departments, identifying specific participants was problematic. Use was made of contacts established at academic and cyber security industry conferences in the three years prior to 2014 to either (a) request their specific participation or (b) request information on who should be approached. One functionary from the EEAS closely involved with the EUCSS had been interviewed for previous research. When approached again, they were amenable to participating a second time. An email was also sent to the contact at DG Connect who had provided the initial list of cyber security *acquis*. While this individual was not able to participate personally, they forwarded the request to others in the department and two interviews were secured as a result.

Where specific individuals had not already been approached at conferences, a search of the European Commission's website identified those DG officials who work in cyber security. DG and agency organigrams[17] proved useful in identifying if not specific individuals then specific units within the DG which could be contacted. This was the case with DG HOME. This method of participant identification proved effective and two interviews were secured. Communication with potential participants was conducted via email.

The majority of interviews were not scheduled at this initial point of contact due to the difficulty of arranging meetings in advance with functionaries and participants at numerous international locations across Europe. Once initial contact was made and participation-in-principle was secured the majority of prospective participants requested to be contacted again on, or immediately prior to, the researcher's arrival at their location. This enabled the arrangement of a fieldwork schedule according to these participation-in-principle agreements. On arrival at the various locations, prospective participants were contacted once again and, when a meeting was agreed, were sent a further email confirming the date of the interview. This confirmation also included the interview questions, participant information and a participation consent form, in order to adhere to the University of Glasgow's ethics requirements[18].

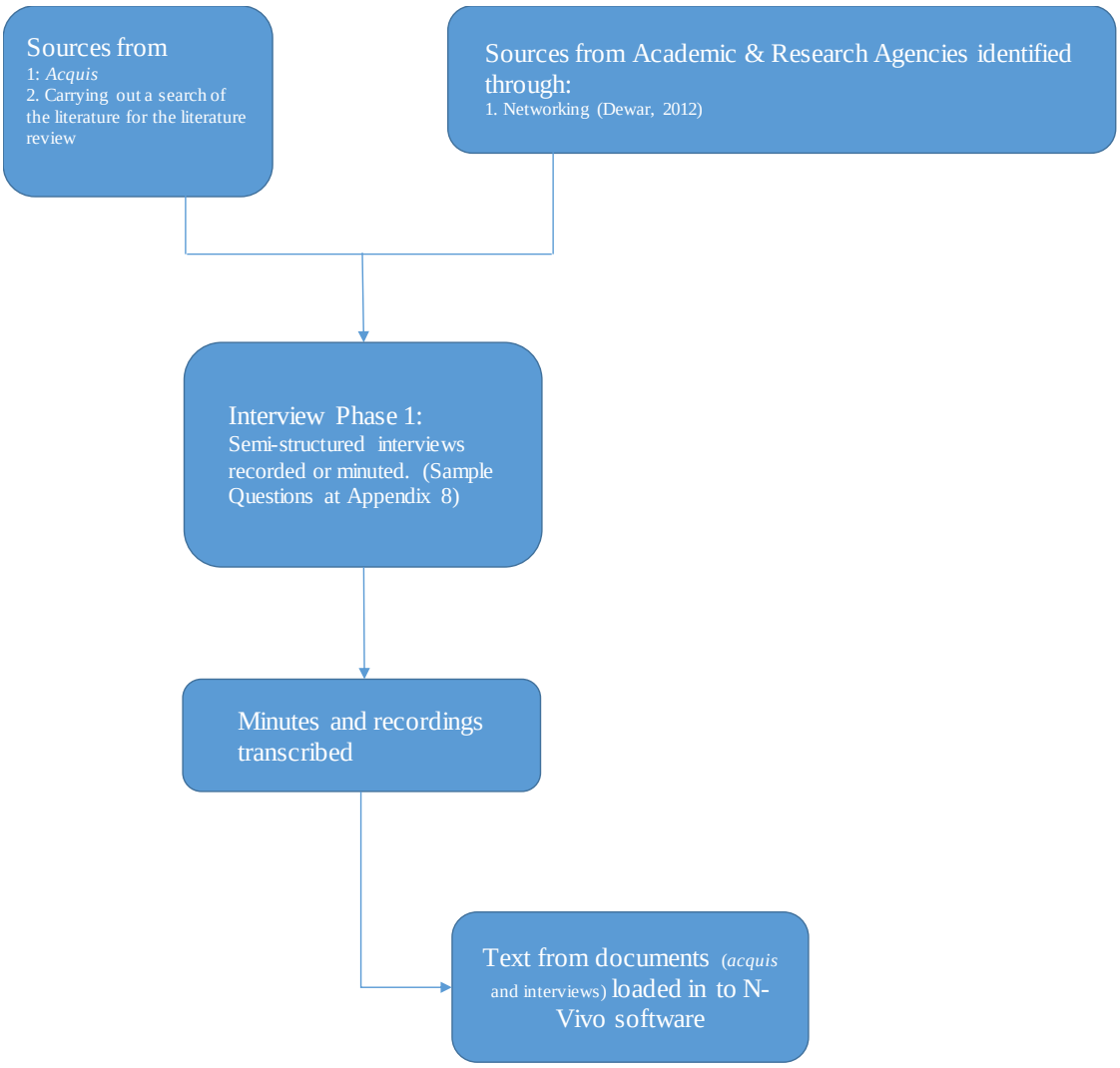
In addition to the initial group of participants identified through the author's own personal networks, further potential participants were identified through a snowball or chain referral system (Burnham et al., 2008, pp. 207–208). As described by Biernacki and Waldorf

[17] The organigram for DG Home is included at Appendices 6 respectively. That for DG Connect is restricted access only.
[18] See Appendices 7, 8 and 9 for sample questions and participant information provided under research ethics guidelines.

(1981, p. 151) a chain referral process is “created through a series of referrals that are made within a circle of people who know each other”. In the case of this research, participants were specifically asked who should be approached for more information in this policy sector. The process proved extremely beneficial, as not only were specific individuals identified who had not been so before, but initial participants could act as gatekeepers and as referees. This expanded the pool of participants considerably, including into areas of difficult access. As Faugier and Sargeant (1997, p. 793) note, “the presence of even minimal contacts may help in the process of selecting and contacting subjects for study in otherwise very hard-to-target populations”. While Faugier and Sargeant cite this as a positive aspect of chain referral in certain areas of social *medical* research, the issue is also relevant when identifying, selecting and securing interviews in sensitive political science research such as this thesis. Chain referral was also beneficial in identifying and securing participants in large bureaucratic entities such as the Commission and when researching a potentially restricted, security-related topic such as cyber security.

In total, 31 interviews were undertaken. The process for acquiring interview participants is summarised in Diagram 3-2 below.

Diagram 3-2: Participant Acquisition Process



3.2.2.2. Conducting the elite interviews – ensuring consistency, fidelity and reliability

To ensure consistency, semi-structured interviews were conducted where each participant was asked the same series of questions (with certain necessary allowances and amendments relating to the specific institution or agency they represented). The semi-structured interview was selected as a data collection tool as certain specific details were needed in order to effect analyses which would assist with answering the research question. For instance, participants were asked which institutional impact was, in *their* view, the most significant in this policy sector, and what was the role of *their* particular organisation or agency in the policy-making process. The semi-structured nature of the interviews

meant that participants could provide their own insights and views which may have been of benefit to this research because an aim of the interviews was to gather data on *other* potential drivers and influences in this policy sector.

In addition to specific questions relating to the main research question, open-ended questions were also posed, designed to enable the participant to freely express experiences, views and opinions on the development process. This facilitated identifying elements not obvious in the primary literature. The aim was to provide participants with the opportunity to "indicate the presence of [other] factors and their effects on individual cases" (Lester, 1999, p. 1) as part of an indicative phenomenological study. Rudestam and Newton (2014, p. 109) state that such amendments and free-flowing conversation are accepted practices in semi-structured interviews of this kind.

To enable as detailed a response as possible, participants were sent questions in advance of the scheduled interview in order that they could prepare. This also facilitated initial contact with subsequent potential participants because subjects were also asked specifically who else should be approached.

The interviews were audio-recorded to facilitate later data analysis and to ensure as high fidelity as possible of the information gathered[19]. To adhere to ethical standards prior permission was sought from the participants to audio-record the interviews. The aim of audio-recording was to ensure that as much information and pertinent data as possible was captured in the interview. As much as 75% of information in an interview can be lost without audio-recording, where the researcher does not possess some form of speedwriting skill (Bucher et al., 1956, p. 359).

Audio-recording of interviews was a very useful tool to ensure the fidelity of analysis to the data and comments gathered from participants. Rudestam and Newton (2014, p. 111) classified recorded interviews as "high fidelity and medium structure", meaning that they enabled the researcher to utilise data representing as accurately as possible the participants' views while also enabling a freer form of conversation and data collection than, for example, a paper-and-pencil test. Audio-recording also enabled the subsequent analysis of comments to be carried out more effectively than by relying on field-notes alone.

Once undertaken, interviews were transcribed *verbatim* into text in order that the same analytical techniques used on primary literature could be applied to ensure consistency of

[19] I.e. to have as accurate a record and account of the views and information provided by the participant.

data collection. The value of audio-recording interviews cannot be understated. Weiss (1995, p. 193) argues that, in data analysis, using anything less than an accurate, high-fidelity transcription of the recording is "playing with the evidence, no matter how benign the intent."

There were a number of limitations with audio-recording. On occasion, permission was given for the recording but restrictions were placed on attribution or citing the participant directly. Similarly, there were interviews where permission to audio-record was withheld. In these instances, field notes were taken and typed-up to provide a digital text document for analysis. As a result, of the 31 interviews undertaken, 29 were referable in one form or another (either anonymously, by institution or by name). The participation consent form included a section on permission for audio-recording[20]. The withholding of permission to record or to attribute did not affect the quality of the data, however. Other recorded and attributable interviews provided enough triangulation of data and results so that there was a minimal reduction in reliability of the data and subsequent findings.

Interviews were conducted during the fieldwork phase of the research study. Funding for this fieldwork was secured from the Centre for Russian, Central and East European Studies (CRCEES) at the University of Glasgow, as well as a successful application for one of four annual overseas fieldwork scholarships from the Universities' Association for Contemporary European Studies (UACES).

The interviews themselves were conducted over two periods. The first consisted of seven weeks in May and June 2014 and was divided between five locations. These were:

- London;
- Athens (which included a meeting at ENISA in Heraklion, Crete);
- The Hague;
- Tallinn;
- and Brussels.

These locations were not arbitrary selections but deliberate choices or delimitations (Rudestam and Newton, 2014, p. 105). They represent the locations of certain national ministries which lead their country's cyber security policy as well as the headquarters of core EU agencies. ENISA is headquartered in Heraklion, and has an operational office in Athens. Europol and the Dutch National Cyber Security Centre are based in The Hague.

[20] See Appendix 9 for a sample participant consent form.

The ICDS and the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) are headquartered in Tallinn.

Brussels was visited last because, as the location of the actors for this study[21], this was the most important location in seeking to understand the development of EU policy. Conducting all other interviews before this portion of the fieldwork provided certain advantages. It enabled chain referral (Burnham et al., 2008, pp. 207–208) to be employed to its maximum potential, and provided the opportunity for participants to identify, or corroborate the identification of, specific individuals in Brussels. It also provided the time to contact and try to secure participation from Brussels-based participants.

Over the course of the first, primary fieldwork period, 29 interviews were conducted. According to Cresswell (1998, p. 64), this total constitutes a "reasonable" sample for a study of this kind, especially considering the high level of some participants in their respective organisation (directors of ENISA for example), and the sensitive nature of cyber security as a policy sector. Josselson and Lieblich (2003, p. 268) argue that a sufficient sample in a social science study of this kind is between 5 and 30 participants. While this number is not based on a precise calculation, it allows for a minimum number of participants required to provide sufficient data for analysis and a reasonable maximum number to avoid saturation (duplicated and redundant results).

Following the data collection and analysis exercise a second tranche of interviews was required as a follow-up. This was conducted solely in Brussels over a period of 1 week in February of 2015. Two goals were achieved in this second period. A number of participants unavailable during the primary tranche were able to be interviewed, and a number of unexpected research findings arising from the analysis of primary literature and interview data – namely the lack of a role for the European Parliament in this sector – were confirmed. Over the course of the two tranches of fieldwork a total of 31 interviews were carried out, with 29 of these being referable and two being completely anonymous and non-referable[22].

As stated above, once the interviews were conducted, audio-recordings and field-notes were word-processed into digital text format. This was in order that the sources could be

[21] The formal institutions of the EU, namely the Commission, European Council, Council of the European Union and the European Parliament. See Chapter 4 Section 4.3.
[22] A full list of referable interviews undertaken is provided at Appendix 10.

uploaded into NVivo software and the same analyses undertaken on both literature and interview sources. Having both primary literature and textual transcripts of interviews helped to ensure the consistency of data collection techniques and the reliability of the resulting data.

3.3. Data collection and Analysis

Once uploaded into NVivo the text-based data sources – *acquis* and interview transcripts – were ready for the main empirical analysis. This raised a methodological problem. Text-based sources and interviews tend to be treated as different types of sources in methodological discussions (Bryman, 2008; Berg, 2004; Hycner, 1985). Because interviews involve direct contact with subjects, data extraction involves the identification of more sociological, linguistic units of meaning from "between the lines" of the participants' statements (Hycner, 1985, pp. 280–294). By contrast, purely text-based sources can be subjected to a content analysis where the occurrence of words and phrases are counted and inferences drawn from the quantitative data.

This raised a methodological challenge. The thesis sought to engage in a fact-finding exercise prior to the important stage of explaining (King et al., 1994, p. 5) policy development processes. On the one hand, therefore, the aim was not to carry out a purely linguistic or sociological analysis. On the other hand, a standard, literature-based content analysis would not have yielded the data necessary to analyse policy development.

In order to analyse both source types consistently, a conceptual content analysis was developed for this thesis. This was achieved by combining methodological techniques developed by Hycner and Berg. Similar ideas, rather than individual words, were identified and counted. Themes, concepts and units of meaning of relevance to the research question were identified and coded (Hycner, 1985, p. 284). This was a similar exercise to a content analysis, but focussed on more abstract concepts rather than individual words. The "counts" of textual elements which characterise content analysis provided a tool for identifying specific units of meaning from which this researcher could learn about participants' views of social phenomena (Berg, 2004, pp. 241–242). The fact that this "Hycner-Berg" technique could be effectively applied to both interviews *and* textual documents made this tool invaluable to this research. It could be applied effectively to both textual primary literature sources such as the *acquis communautaire* and the transcripts of elite interviews.

An additional benefit of employing a conceptual rather than standard, metric content analysis became apparent because different words and phrases were used to describe the same elements and concepts over the course of the 28 years between 1985 and 2013. An example of this is the term "cyber security". This term was used in Union *acquis* from 2002 onwards. In the preceding years terms such as "online security", "network and information security" and "online" or "internet safety" were used interchangeably to refer to the risks, threats, concerns and issues which comprise cyber security in its most recent iteration. Conducting a standard content analysis, where the occurrences of specific words are counted, would therefore miss out occurrences of the same concept, where *different* words were used in their description.

3.3.1. Generating Data: Coding the *acquis* and interview transcripts

The first step in the data analysis process was to generate a coding schedule to be applied to all text-based sources – the primary literature and interview transcripts. This coding schedule would comprise key concepts to be sought in all text sources and reflect the aims of the research. Institutional drivers, actor participation and non-institutional elements would be identified and coded.

Because the research sought to identify the institutional drivers behind a specific policy sector – cyber security – a control schedule was generated by conducting a content analysis of the EU's *Cyber Security Strategy* (EUCSS). In order to understand the development of the EU's policy choices, it was first necessary to identify which processes and concepts were most relevant to that policy. Because the EUCSS represented the sum total of the EU's policy choices and the end-point of its development process, it contained the elements which could be sought in preceding policy documents that would explain the development process. This was achieved by conducting an open coding of the EUCSS.

This action yielded a schedule of 43 discrete codes, labelled "nodes" in NVivo software. Some of these nodes referred to similar concepts, but involved separate entities. For example, co-operation between EU Member States or co-operation between EU agencies were similar but coded separately. These discrete nodes were collated into what Hycner (1985, p. 287) labelled "clusters". From 43 separate nodes, 16 clusters were distilled. Some clusters contained only single nodes. Others such as "facilitation" contained as many as seven. The purpose was to derive, as closely as possible, collective units of

meaning referring to what Berg (2004, p. 239) described as the unit's essence or *telos*[23]. They facilitated the identification of latent content. This is data inferred from the words used. It contrasts with manifest content, where information is specifically expressed (Berg, 2004, p. 242). These thematic clusters would be sought in the complete library of text sources. The complete NVivo node list – i.e. the digital control coding schedule – is available at Appendix 11.

Coding the data sources according to the control schedule involved reading *acquis* and transcripts to identify units of meaning in the conceptual content analysis. This reading led to the identification of a number of further ideational and institutional elements found in the *acquis* and interviews, but which were not set out in the EUCSS. Due to the prevalence and recurrence of these elements, two further supplementary coding schedules were initiated: one for *acquis*, the other for interviews. All *acquis* and interview transcripts were thereafter coded three times, first with the EUCSS control and then with the two non-EUCSS coding schedules. This exercise ensured the capture of as much relevant data as possible relating to the research question. The non-EUCSS schedules are provided at Appendix 12.

As with the control schedule derived from the EUCSS, the units of meaning derived from the *acquis* and the interviews were arranged in thematic clusters. It should be acknowledged at this point that a degree of the researcher's own judgement was employed to determine whether or not two or more units of meaning were synonymous due to the inconsistent use of terminology. This is a potential limitation in the data collection process. According to Hycner (1985, p. 288), the researchers' own suppositions may generate a bias in the resulting data. In the case of this thesis, this potential bias from the researcher's presuppositions could be minimised. This was achieved by developing clusters and synonyms derived from specific sources in the texts and *verbatim* statements in the interviews, rather than the researcher projecting an inference or interpretation of what was meant in, for example, an interview.

Two additional activities were employed to enhance the reliability and validity of data. The first was further eliminating redundancies once the coding was completed (Hycner, 1985, p. 286). While care was taken throughout the data collection process to avoid duplication of nodes or synonymous concepts, similar units of meaning were inadvertently identified and coded separately. To ensure the transparency, reliability and validity of the

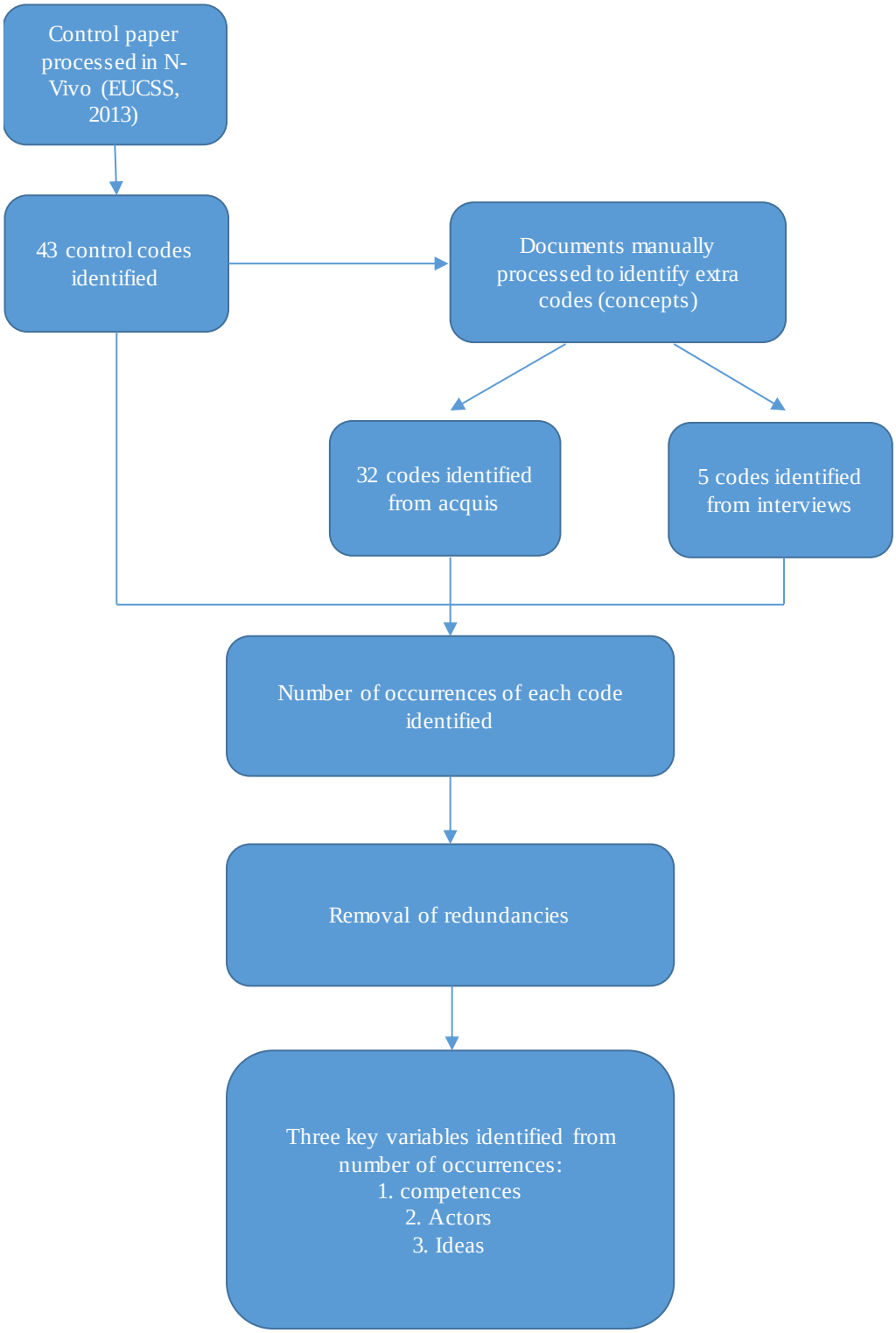
[23] This is similar to the Platonic base "form" of a concept.

data collected, a “clean-up” of the NVivo nodes (the CAQDAS codes and units of meaning) was undertaken prior to examination and analysis of the results. This clean-up clustered together or corrected synonymous concepts to ensure as little aberrant duplication as possible. The final data set was as free from duplication redundancies as was possible to achieve.

To further enhance data reliability and validity, triangulation was also employed. Triangulation is a corroborative technique which involves the use of several methods or sources at once “so that the biases of any one method might be cancelled out by those of the others” (Seale, 1999, pp. 472–473). Tarrow (2010, p. 108) argues that triangulation is a useful tool for the corroboration of findings derived from both qualitative and quantitative data collection techniques. Findings from the primary literature – such as the preference for the EU towards facilitating co-operation – were also identified independently in certain of the elite interviews. Such triangulation exercises increased the reliability of the findings by reducing the reliance on one particular type of data source.

The process by which data was generated is summarised in Diagram 3-3 below.

Diagram 3-3: Data generation process (coding)



Following the conceptual content analysis exercise undertaken to extract data from the *acquis* and interview transcripts, those data were tabulated according to the most frequently occurring elements. What was being sought were the actors most frequently involved in the policy-making process, the institution of greatest influence in this sector

and the most frequently occurring non-institutional elements. To effect an HI analysis these three details were required to be identified over the entire course of the timescape. Specifying actors, institutions and elements in this manner would concentrate the analysis on the interaction of those three aspects *over time*, a key component of an HI analysis. These data tables are presented in the empirical chapters of this thesis.

The quantitative exercise outlined above was vital in preparing data for a more qualitative analysis. As Goldstone (1991, pp. 50–62) states:

> To identify the process, one must perform the difficult cognitive feat of figuring out *which* aspects of the initial conditions observed, in conjunction with *which simple principles* of the many that may be at work, would have *combined* to generate the observed sequence of events. (emphasis in original)

Any institutional analysis of policy development must first identify which institutions and actors are relevant in the sector under examination. This identifies who and what are involved and of importance to the policy development process. Once this has been achieved, how and why they are involved can be investigated. To achieve this, a qualitative narrative inquiry approach was employed.

3.4. Narrative Inquiry: Employing HI techniques

The content analysis exercise outlined in the previous section identified which institutions and ideational elements were most at work over the course of the timescape. The next stage of the thesis involved examining *how* these elements influenced the development of the EU's discourse in this policy sector. This formed the bulk of the analysis required to answer the research question. Analyses examining the totality of the timescape between 1985 and 2013 looked at the inter-relationship of the institutions and ideational elements to chart their interplay over time (Pierson and Skocpol, 2002, p. 3). As Thelen and Steinmo (1992, p. 13) state, the purpose of institutionalism "is to demonstrate the relationships and interactions among a variety of [elements] in a way that reflects the complexity of real political interactions". The results of this analysis form the empirical chapters of this thesis.

To effect this analysis a complex-form, detailed narrative inquiry was conducted. This was achieved by chronicling the interaction and influence on policy of the institutions, actors and non-institutional elements to "identify the causal chain and causal mechanisms – the causal process" (George and Bennett, 2005, p. 206). Narrative inquiry involves examining social phenomena and experience over time (Etherington, 2013, p. 3). Studies employing

narrative inquiry tools "have temporal dimensions and address temporal matters: they focus on the personal and the social in a balance appropriate to the inquiry: and they occur in specific places or sequences of places" (Clandinin et al., 2000, p. 54). Because of the focus on these temporal considerations, narrative inquiry lends itself to an historical institutionalist analysis.

The first task was to extrapolate from the quantitative data the occurrences of the institution, actors and non-institutional elements. These three elements were then identified in each of the core cyber security documents published between 1985 and 2013. These results were tabulated to show their occurrence and interaction over the timescape. It also facilitated the analysis of their interaction in their historical context at key points in the timescape. This meant that the interaction of these elements was examined *in time* rather than merely over time (Bulmer, 2009, p. 307).

Bennett and Checkel (2015, p. 6) provide an analogy for this type of study. Although they use it to refer to process tracing, the analogy fits a narrative inquiry approach. They liken it to a row of 50 dominoes lying after they had previously been standing. Merely looking at the dominoes only provides a start and an end point. It does not provide any information "about whether the first domino caused the last to fall through a domino process, or whether wind, a bump of the table or some other force caused the dominoes to fall". They argue that evidence relating to that intervening process must be gathered so that it can be fully understood. Analysing the interaction of institutions, actors and non-institutional elements in their historical context provides these insights into the process by which the EU's cyber security policy was developed.

3.5. Reflections on methodological strengths and limitations

3.5.1. Methodological Strengths

The combination of source types – interviews and primary literature – served to provide a rounded, holistic body of data for analysis. Elite interviews and *acquis communautaire* functioned in a symbiotic relationship to provide data for a narrative inquiry approach which uncovered the interaction of elements crucial to policy development. The Union's *acquis* is a finished product. It represents the end-point of policy development. What it lacks, however, is insight into the process of development. This is the focus of this research. Elite interviews with functionaries and officials intimately involved with that development provided this insight. Participants were able to shed light on internal

machinations and ideational drivers which affected particular decisions and policy choices. Just as an analysis of EU policy cannot be undertaken without recourse to the *acquis*, an analysis of EU policy *development* cannot be undertaken without examining the background processes not presented in that *acquis*.

Utilising both primary literature and elite interviews necessitated the development of a conceptual content analysis. This allowed both source types to be analysed using the same techniques, a methodological tool which increased the validity and reliability of data gathered. Analysing two separate source types in the same manner reduced the likelihood of data redundancies and errors by treating all sources equally. The identification of institutions, actors and non-institutional elements identified from two sources treated in the same manner is therefore more reliable.

The research methodology also successfully used a mixed-methods approach. While quantitative data was extracted to identify important institutional and non-institutional elements, a qualitative narrative inquiry was conducted to examine the interaction of those elements. The object of the research is to understand the institutional dynamics behind the EU adopting a particular policy approach. Simply identifying the institution of relevance in a quantitative analysis only partially answers the research question. Applying a complex-form, detailed narrative inquiry approach where the interaction of those elements is examined over time and in their historical and political context provided a more nuanced, clear and complete understanding of the developmental processes involved.

3.5.2. Limitations

There were certain limitations to the research methodology (Rudestam and Newton, 2014, p. 105). One such limitation was encountered when identifying core elements of the study. The identification of actors most relevant to cyber security could be carried out through the collection and categorisation of *acquis*, with triangulation being effected through interview data. Identifying the most important institution(s) was more problematic. According to Hall (1992, p. 96), institutions are the standard operating procedures, patterns of behaviour and rules within which actors in complex political systems interact. In the EU these rules are many and varied. They range from the system of voting in the Council of the European Union when passing legislative proposals or the rules governing the length of time the European Parliament has to consider strategy proposals from the Commission, to the general competences of the Union as a whole. Identifying a specific rule or system of behaviour which has greater or lesser significance in a single policy area was a significant

challenge for this research. This challenge was exacerbated by the fact that Union *acquis* does not specify which one of these myriad rules was most at work in a specific document.

To resolve this challenge, interview participants were specifically asked which institutional influence – which set of procedures or rules – was the most important in EU cyber security policy development. The responses indicated that the competences were the most important aspect governing why the EU does what it does *vis-a-vis* cyber security. On the face of things the concept of Union competence is simple: "what the EU can or cannot do" (Bache et al., 2011, p. 248). Union competences not only spell out in which policy areas the EU can become involved but also to what extent.

One problem did arise with this exercise. The interviews undertaken tended to concentrate on the final years of the policy-making timescape. This was due primarily to the tenure of EU bureaucrats and functionaries at their various posts. It was not possible to interview a functionary who had been in position for the duration of the 28 year timescape. The EU itself had undergone a number of significant structural changes in that period and each actor had evolved. Policy sectors had developed and individuals moved from one sector to another. Those interviewed for this research understandably had better knowledge about the most recent developments than the entire timescape. Another reason for analysing primary literature and interviews using the same technique was that this mitigated the temporal specificity of those interviews. Details could be gathered from the historic *acquis* which could not be gleaned from interviews with participants more recently involved in the process. This is not to say that the interview data is deficient. It is merely to acknowledge that there is a time-limited nature to the data derived from interviews due to the periods for which interview participants were in office.

The time-specific nature of the interviews posed a problem for triangulation, however, given that the timescape of this thesis is the 28 years between 1985 and 2013. Due to the natural turn-over of staff in the institutions, agencies and bodies, selected participants were not party to the full policy-making timescape. Deliberations and choices of the pre-2007 period corroborating statements for this earlier timeframe were particularly problematic.

To overcome this, a three-stage process was employed to provide corroboration for the earliest periods of policy development, those prior to 2007. The independent interviews from academic and research institutes, EU functionaries and national representatives had already provided triangulation for identifying Union competences as the most important institutional driver in this field in the post-2007 period. To find corroboration relating to

pre-2007, *acquis* from this period was analysed to find evidence for competences directly influencing policy-making. The first step to achieving this was to identify what the competences were at that time. At the earliest point in the timescape, the Single European Act (SEA) of 1987 and the Maastricht Treaty of 1992 established the framework for EU action. The SEA limited Union capabilities in security matters to political and economic aspects of security (European Union, 1987, p. 1049) while the Maastricht Treaty confirmed wide competence for the EU in economic and social affairs, and more limited competence in criminal justice and foreign policy (Bache et al., 2011). This established a base-line of competence for the earliest phase of the cyber security policy-making timescape[24].

The second step was to employ a hoop test to analyse Union *acquis* documents from this period to identify whether these competences had any influence on their development. As a result of a desire to boost economic growth and reduce unemployment, the burgeoning ICT sector had been co-opted as a core element of the Single Market Programme (SMP) (European Commission, 1985, p. 20). The management and development of the SMP was also subject to the socio-economic competences of the EU as set out in the SEA and the Maastricht Treaty. This meant that, logically, cyber security was also subject to those same competences. Although the competences required to be confirmed only once, this triangulation with the *acquis* was repeated in later phases and provided corroboration of the influence of Union competences on cyber security over the period of the timescape *not* covered by the interviews.

The consequence of this two-step exercise was that Union competence could, with a certain degree of confidence, be established as the institutional dynamic with the greatest influence on the development of cyber security policy in the EU. The combination of triangulation of interview data from the period 2007-2013 with the hoop test exercise relating to earlier, pre-2007 periods provided support for this conclusion where interview data was sparse.

Other limitations encountered were of a more practical nature. Certain of the interviews were not audio-recorded and two were held completely off the record, including one at a very high level within the EU. As a result the data from this interview could not be put to as full a use as other, recorded, sessions. While of limited benefit to the data collection and analysis of this research, the interview was beneficial for establishing a context for the

[24] This exercise was made much easier by the fact that no major changes to Union competence were undertaken between 1992 and 2009, when the Treaty of Lisbon entered into force. Competences needed only to be confirmed once.

EU's policy in this sector, and illuminating certain aspects of actor interaction at high level. This corroborated certain findings and provided useful background for the main analytical activities, while enabling permissions from participants, or the lack thereof, to be respected. This is an important ethical consideration.

There were also practical limitations which affected the collection and collation of Union *acquis*. The hoop test and cataloguing exercise identified publicly available policy instruments. However, there were at least three documents not included in the compiled library. This was due to issues of access. Two documents were not available in a digital format in the first instance and hard-copies could not be located. An access request to the Council of the European Union Secretariat for the third document was refused. This means that the thesis utilised all *possible* available literature, while acknowledging that this collected library did not include *all* the relevant *acquis communautaire*. Nevertheless, those documents which were examined included those of greatest significance to the policy development process. Thus, a level of literature inclusion was attained that enabled a reliable analysis.

While it is important to acknowledge access issues when conducting policy research, in this instance such issues did not affect the quality of the analysis. It is always beneficial to have access to all the documents pertaining to a policy area. However, this thesis is an historical institutionalist analysis which examined a policy in a period prior to digitisation. The collection techniques and resulting library of policy documents was deemed, if not complete, then as comprehensive as possible in order to conduct an effective analysis.

It is also beneficial to acknowledge the inconsistent use of terms in a field which was itself rapidly evolving. Terms such as "cyber security" only began to be used midway through the timescape, but, through a process of retroactive continuity[25], have been applied to all areas of online safety and security throughout the timescape. To resolve this issue and mitigate its limitation, a conceptual content analysis, rather than a standard word-count, was conducted to identify synonyms. A subsequent clean-up exercise was undertaken to remove redundancies and false positives. While this is also a form of retroactive continuity and is not fool-proof, this combination of techniques reduced the impact of multiple terms for conceptually similar ideas.

[25] See Section 1.5.2.1.: Retroactive Continuity: Applying modern terms to historic concepts

3.6. Conclusion

This chapter set out the research design, methodology and ethical considerations required in order to collect data for this thesis and conduct a suitable analysis. Data was collected from two source types: EU *acquis communautaire* and elite interviews. These complemented each other as important data regarding policy development could not be gathered from *acquis* analyses alone.

While primary literature sources were collected from online databases and physical libraries, interviews were secured at the European Commission, the Council of the EU, the European Council and the European Parliament. These were the four institutions most relevant to this research. In addition, interviews with specialists from a number of research organisations and academic institutions were also secured. To ensure ethical considerations were maintained, interviews were audio-recorded but only when permission was given.

A conceptual content analysis based on a combination of Hycner and Berg's analytical methodologies was also developed. This enabled both source types to be analysed in the same manner using NVivo CAQDAS software. Doing so increased the reliability of the data collected as there were fewer redundancies caused by using different collection methods.

There were a number of strengths to this methodology and research design. The use of both interviews and *acquis* meant that not only was it possible to establish a complete picture of policy development, triangulation of findings was also possible. This was particularly beneficial given the temporal nature of the research. Findings from the earliest points in the timescape could be triangulated and corroborated with information from later stages.

That temporal nature also yielded certain limitations. It was not possible to interview functionaries who worked on policy at the earliest points in the timescape. Due to the changing nature of the EU itself, as well as time-limited placement of functionaries at the EU's institutions, there was no-one who had been in post continually between 1985 and 2013. In addition, certain of the interviews were not audio-recorded due to permission being withheld. A final limitation to overcome was the inconsistent use of key terms such as "cyber security". Although this could to a certain extent be mitigated by the process of

retroactive continuity, a conceptual content analysis technique, rather than a standard word count, was employed to ensure that conceptually similar terms were identified.

The methodology for this research therefore employed a mixed-methods approach to gather sources and data as well as conduct analyses of that data. While a number of techniques were derived from previously conducted studies, such as adapting Hycner's model for phenomenological studies, the combination of methods employed enabled the identification of actors, institutions and non-institution elements. It also enabled an effective analysis to be carried out in order to provide an answer to the research question. The following chapters – the empirical section of the thesis – set out and examine the results of this data collection and analysis process.

Chapter 4 | Theoretical Framework: Applying Historical Institutionalist Elements and Functions

4.1. Introduction

This chapter explains how historical institutionalism (HI) will be applied in this thesis. As set out in Chapter 1, three mechanisms of HI postulated by Pierson and Skocpol (2002, p. 3) will be used to frame the research and analyse the data gathered. Pierson and Skocpol argued that HI techniques address

> ***big, substantive questions that are inherently of interest to broad publics as well as to fellow scholars***. To develop explanatory arguments about important outcomes or puzzles, historical institutionalists ***take time seriously***, specifying sequences and tracing transformations and processes of varying scale and temporality. Historical institutionalists likewise ***analyze macro contexts and hypothesize about the combined effects of institutions and processes*** rather than examining just one institution or process at a time. Taken together, these three features – substantive agendas; temporal arguments; and attention to contexts and configurations -- add up to a recognizable historical institutional approach that makes powerful contributions to our discipline's understandings of government, politics, and public policies. (Emphasis in original)

The question this thesis will answer – the *substantive question* – is: have institutions and institutional arrangements led the EU to develop and continue with a socio-economic approach to cyber security? This question will be answered by analysing the effect of institutional forces over a period of 28 years, therefore *taking time seriously*. Finally the thesis *hypothesizes about the interaction of institutions and processes* in the specific sector of cyber security policy. As set out in Chapter 1, the third supplementary question the thesis will answer examines the influence of the interaction of institutional frameworks and non-institutional elements on policy continuity. In order to employ these HI mechanisms successfully, it is first necessary to clarify the institutions and actors which will be studied.

This chapter will first set out the institutions which will be studied in the thesis. This is important because the term "institution" is an ill-defined concept (Scharpf, 1997, p. 38). Conceptualisations range from enduring, stable patterns of behaviour and cognitive structures (Huntington, 1968, p. 12; Smith, 1988, p. 91) to wider collections of behaviours, norms and standard operating procedures (March and Olsen, 1989, pp. 21–6).

This thesis will adopt Hall's (1992, p. 96) definition of institutions as "formal rules, standard operating procedures and customary practices" which affect actor behaviour and

effect policy choice. In the case of the EU, the rules, procedures and practices for policy-making are underpinned by its Treaty-defined competences. Union competences dictate the manner in which actors interact, with which procedures they develop policy and in which policy areas the EU is able to operate. Any research seeking to understand the policy-making process and choices made in a specific field will therefore need to examine the effect of Union competences on that policy field.

After clarifying that the collection of Union competences is the institution of greatest relevance to the thesis, the chapter will set out the actors who operate according to those competences. In doing so, a variation to traditional studies of the European Union will be posited. Such studies focus on the actions of the Member States and political groupings within the EU's seven formal institutions. This is logical given that most theories of IR, such as realism and liberalism, place the sovereign state at the highest level of action. This thesis will instead adopt Scharpf's (1997, p. 52) definition of "composite actors" in order to consider the formal institutions of the EU as actors operating within the institutional setting of Union competences.

To support this departure from academic conventions, the "actorness" of these entities will be tested by applying Bretherton and Vogler's (2006, pp. 24–35) three-step framework – presence, opportunity and capability. The chapter presents the argument that the institutions are actors due to their presence within the structure of the Union, their capacity to effect policy decisions and change, and the existence of opportunities to do so. The chapter therefore shows how Bretherton and Vogler's framework of "actorness" was combined with Scharpf's definition of composite actors to create a new "Scharpf-Bretherton-Vogler" conceptualisation or model of social actor. This new model will be applied to the formal institutions of the EU to further evidence their role as political actors.

Using this categorisation of "composite actor" will be beneficial in helping to understand the reasons why the EU rather than its Member States made particular choices in cyber security. It will also facilitate a more nuanced understanding of policy development within the over-arching institutional structure of the EU. Finally, it resolves potentially confusing issues of nomenclature when referring to the EU's "formal institutions" within an institutionalist analytical framework.

The chapter will also look at two important functions common to HI and the study of social and political phenomena and how they relate to this thesis. The first is path dependency. The fundamental premise of path dependency is that decisions made when an institution or

policy is initiated have an ongoing influence into the future (Peters, 2005, p. 70). Although this is a deceptively simple idea, as both Mahoney and Peters argue (Mahoney, 2000, p. 507; Peters, 2005, p. 70), it is a core function of HI study and a useful tool for explaining decisions made in the later stages of a policy timescape. If a policy path remains in place long after its establishment, the case can be made that the choices made at the commencement of the policy path dictate the nature of that path.

The second function which will be employed to analyse EU cyber security policy over time is closely related to path dependency. While path dependency can explain policy continuity, the concept of "punctuated equilibrium" can explain policy change. Punctuated equilibrium refers to a significant force intervening to amend a policy path or divert it from an established direction (Peters, 2005, p. 21).

The chapter is divided into five sections. Following this introduction, the second section of the chapter will clarify the institution which will be studied in this thesis. The third section will set out which actors are relevant to the analysis. The fourth section will look at the influence of path dependency and punctuated equilibrium on the analysis while the fifth and final section will provide some concluding remarks on the selection of HI as the theoretical framework for this research.

4.2. The institutions relevant to this thesis

This thesis takes as its starting point Hall's definition of the term "institution". Hall describes institutions as "the formal rules, compliance procedures and customary practices that structure the relationships between individuals in the polity and the economy" (Hall, 1992, p. 96). The term "institution" therefore includes systems of norms and accepted patterns of behaviour that become entrenched in an interactive, political system, as well as bricks-and-mortar, existent organisations (Bannerman and Haggart, 2014, p. 10). Hall's definition has been chosen for this research because of this breadth of meaning. The European Union is itself an existent institution made up of agenda-setting bodies and operational agencies. However these groups and agencies interact according to a complex system of norms, patterns of behaviour, compliance procedures and customary practices. This system is underpinned by the EU's competences. These competences set out the policy areas in which it can operate, and the extent to which it can involve itself in those areas.

This is an important contribution to EU studies and the field of cyber security. The analysis of the *influence* of abstract institutions such as norms and standard modes of behaviour on EU cyber security policy has not been carried out. As examined in the Chapter 2.3, HI analyses of EU policy tend to focus on the influence and interaction of existent bodies. This thesis seeks to understand the influence of more abstract institutional forces on policy-development.

4.2.1. Classifying Union Competences as an Institution

The capacity for the EU to engage with particular policy fields is a closely governed and monitored aspect of its structure (Bache et al., 2011, pp. 248–50). The areas in which the EU becomes involved, and the manner of that involvement, are governed by Treaty-defined competences. As Bache, George and Bulmer point out (2011, p. 248), the concept of Union competences is relatively simple: it refers to what the EU can or cannot do. Prior to the entry into force of the Treaty of Lisbon in 2009, this capacity was governed by the principle of subsidiarity. This is the concept whereby decisions should be made as close to the level of the citizen as possible, except where it makes more sense to handle an issue at national or European level (European Union, 1995; Follesdal, 2013, p. 1). As Kersbergen and Verbeek (2007, p. 225) argue, this meant that:

> The European Community (Union) can only justifiably legislate and pursue policies in areas that fall exclusively within its competence, if the Member States are incapable of acting adequately on their own or if the scale and effects are such that the Community (Union) can achieve the objectives more effectively.

Transnational issues such as the customs union or the common agricultural policy were handled at the EU level for the simple reason that it made sense to do so.

The simplicity of this definition is deceptive, however. The reality is that Union competences are a complex set of rules separating policy areas and specifying levels of Union and Member State involvement in those areas. It even leads to differing voting procedures and requirements, depending on the subject under discussion. Under Article 3 TFEU, the EU has **exclusive** supranational competence in the areas of the customs union, Eurozone financial matters, establishing competition rules for the internal market and conservation of marine resources under the common fisheries policy (European Union, 2009a, p. 51). The EU **shares** competence with national Member State governments in areas such as wider internal market policy, the environment, the area of freedom, security and justice, energy policy and consumer protection (European Union, 2009a, p. 51).

Finally in measures relating to areas such as health, industry, culture and tourism (European Union, 2009a, p. 52) the EU can only **support** national governments. Supporting competence is the weakest form of EU operational capacity.

To further complicate the matter, security competence is defined elsewhere. The Single European Act of 1987 restricted the EU in its capacity to act and develop policy in security matters. It categorically stated that the EU can only involve itself in political and economic aspects of security (European Union, 1987, p. 1049). This restriction has never been lifted and remains a red line for members of the EU. It means that national security matters remain the responsibility of the Member States. As a result there is a separate, unofficial category of "**special competence**" (European Union, n.d.) relating to the Common Foreign and Security Policy (CFSP). This means that the CFSP is

> characterised by specific institutional features, such as the limited participation of the European Commission and the European Parliament in the decision-making procedure and the exclusion of any legislation activity (European Union, n.d.).

CFSP policy is defined and implemented exclusively by the European Council and by the Council of the EU. This has particular implications for cyber security given the need to reconcile the potential national security implications of large scale cyber incidents with the inherent transnationalism of digital networks.

This division of competences is a crucial operational practice and "institutional factor" (Hall, 1992, p. 97). It establishes and governs patterns of behaviour and interaction of the key actors involved in policy-making. The combination of defining policy areas and levels of involvement means that the competences define the very nature of the European Union itself and describe the basis for all EU functionality. The competences organize policy development "into something more than a seamless flow of activities and events" (Orren and Skowronek, 1996, p. 111). Union competences will therefore be studied over time in order to identify their long-term influence on cyber security policy-making.

It should be noted that special care must be taken when examining the institutional role played by Union competences in the context of policy development. The patterns of behaviour and standard operating procedures established by the competences affect *all* areas and aspects of EU policy, Member State behaviour and interaction, and the political structure of the Union itself. This is important because, in one respect, the answer to the research question is simply that the Treaty-defined competences dictate what, how and why the EU does what it does. This includes establishing the parameters for tackling

"computer crime", the term in the Treaties most analogous to cyber security (European Union, 2009a, p. 81). Evidence for the importance of the competences comes from the *acquis* and interviews undertaken for this thesis. Eleven of the 31 interviews carried out during fieldwork specifically cited Union competence as the institution of greatest influence on cyber security. Comments from EU officials stated that the reason the EU has adopted a socio-economic cyber security policy is due to the restrictions placed upon it by its competences (Interview, Senior Official, DG HOME, European Commission, 2014; Interview, Senior Official, DG MARKT, European Commission, 2014; Interview, Senior Official, EEAS, 2014).

This answer belies the complexity of the institutional effects of the competences on policy development, particularly in the field of cyber security. The interview data cited above presents evidence of what the influence of the competences on EU cyber security policy *was* in the run-up to the publication of the 2013 EUCSS. It does not explain *how* or *why* they had the influence they did. This is needed in order to identify and understand the precise institutional influence of the competences in relation to the research question for this thesis. There is considerable fluidity in terms of *how* policy is engaged with. The remit and scope for action *within* a policy area is very broad despite the competences, as set out in the Treaties, appearing to restrict the Union to a specific, prescribed set of policy fields with certain no-go areas such as national security and defence. In other words the EU can, and does, do a great deal while remaining within the confines of its competences (Interview, Senior Official, DG HOME, European Commission, 2014). For example, while retaining shared competence in Internal Market affairs, the European Commission has a right of initiative in this field. It can propose legislation and policy in any area affecting the Single Market without waiting for instructions or requests from the Parliament, the Council of the European Union or the European Council. As a result the EU can be involved in a huge range of issues, from personal privacy (European Commission, 1992a; European Parliament and Council of The European Union, 2002) to establishing secure industrial systems (European Commission, 2006b, p. 8).

An influence of the competences is that they govern *how* the EU can approach an issue. In order to become involved in a security matter the Union must approach these issues from a socio-economic standpoint. This is what the EU has done in cyber security policy. The threats and risks emanating from cyberspace have an overt national security element when, for example, critical information infrastructures are threatened or targeted. The EU can interpret these issues as risks to the ongoing functionality of the Internal Market and hence

tackle the risks to that functionality. As will be demonstrated in Chapter 8 below, the EU's response to instances of inter-state aggression in cyberspace such as the attacks on Estonia of 2007 prioritises these incidents' impact on the EU's capacity to function as an economic entity. The primary referent object of cyber security policy is the economic and financial functionality of the Single Market and the citizens who live and work within it.

This fluidity of action *within* the institutional confines of Treaty-defined competences is of vital importance to this thesis as it provides a potential answer to the primary research: the competences of the EU necessitated a particular interpretation or construction of cyber security risks and threats which led to the EU developing its idiosyncratic, socio-economic approach to those threats. This research seeks to expand on this partial answer, and identify and understand the influence of competences on the development of cyber security policy. In addition, the thesis seeks to understand any correlation between the competences and the continuation of the EU's socio-economic cyber security narrative.

For the purposes of this research, therefore, the institutions to be examined are the competences of the EU. The empirical data analysis will seek to clarify the influence of Union competences on cyber security policy. It will examine why and in what manner the competences necessitated particular policy choices in this field.

4.3. Actors for this study – clarifying "actorness"

In an HI analysis it is also necessary to define the actors operating within the institution under examination. Current EU scholarship traditionally considers the Union's Member States to be the actors operating within a particular institutional setting (Bulmer and Padgett, 2005; Pierson, 1996). An example of this is Bulmer's (2009) examination of the evolution of the European Coal and Steel Community (ECSC) into the present European Union. This study focussed on the relationship between the supranational institutions of the EU and the Member States. This thesis, however, will consider the seven formal institutions of the EU – the European Commission, the European Parliament, the Council of the European Union, the European Council, the Court of Auditors, the Court of Justice and the European Central Bank – as the actors whose choices will be examined.

There are two reasons for considering these bodies as actors. The first reason is that this thesis seeks to understand why the European Union and not the Member States developed a particular cyber security policy. To do this it is necessary to examine policy development in the context of the interaction of the formal institutions of the EU. That

interaction occurs according to the formal rules, compliance procedures, customary practices and norms defined by Union competences. Within this context, each formal institution operates as a single, gestalt entity.

The second reason is a matter of practicality concerning nomenclature. The term "formal institution" has particular legal meaning when discussing the bodies of the European Union. The term refers explicitly to the seven principal, organisational bodies listed above. Referring to these entities as "institutions" in an institutionalist analysis can lead to confusion. By considering these entities as actors, and referring to them as such, this confusion is avoided.

To further justify the consideration of these bodies as actors, the thesis will adopt Scharpf's (1997, p. 52) conceptualisation of "composite actors". Scharpf argues that entities with an intentional capacity over and above the individuals which comprise them are better described as composite actors, entities with their own preferences and strategy choices. The reasoning behind this argument is that such gestalt entities – for example the European Council or the European Commission – are existent organisational bodies with an independent capacity for purposive action: they have a life and "actorness" of their own. Such a term suits the formal institutions of the European Union. Within the architecture of the EU these entities have specific purposes and roles which influence the choices and actions of the others. Furthermore, there is a capacity for one actor, such as the European Court of Auditors, to hold another to account, further emphasising the independence of those entities within the EU context.

This conceptualisation of composite actors lends itself to the analysis in this thesis as it will examine the internal machinations of the Union itself in which the Commission, Parliament *et al* take part, rather than the actions of Member States within the European Council, party political groups within the Parliament or potential business interests within the ECB. In addition, the use of the term "composite actor" resolves the difficulty of nomenclature by not employing the confusing term "formal institution" in an institutional analysis. Such a resolution more accurately portrays these bodies' functions and roles in the EU policy development process and internal Union architecture.

Further support for considering these "formal institutions" as actors can be found in Bretherton and Vogler's (2006, pp. 24–35) framework of "actorness". Although this framework was designed to provide evidence and support for the notion that the EU as a

whole is an actor on the global stage, the framework can be effectively applied to the "formal institutions" of the EU.

4.3.1. Defining "Actorness"

According to Bretherton and Vogler, the definition of an actor in international relations hinges on an entity's presence, opportunity and capability to act in the circumstances under examination. The seven "formal institutions" of the EU are existent bodies, constituted by Union Treaties. These Treaties confer on these bodies a presence in the policy process. They establish their parameters of action within the policy development process and also identify them as contributors to that process in their own right. As such presence does not necessarily equate to purposive action, but is "a consequence of being" (Kaunert and Zwolski, 2014, p. 595).

Opportunity is defined by Bretherton and Vogler as "the context which frames and shapes EU action or inaction" (Bretherton and Vogler, 2006, p. 24). In other words, there needs to be a policy area or issue in which the entity can act. The "formal institutions" of the EU, in particular the European Commission, are tasked with ensuring that availability. In the field of cyber security, opportunity for the "formal institutions" to act is provided by the need to ensure the security of the pan-European ICT infrastructure in the context of its relevance to the internal market. The European Council had the opportunity in the late 1980s and early 1990s to take action to ensure that viability by tasking the Commission with formulating concrete proposals to boost jobs and growth. One of the resulting avenues was through the promotion of ICT.

Finally, the EU's entities need more than a reason and an opportunity to act. They must also have the capabilities to do so. They must "capitalise on presence and respond to opportunity" (Bretherton and Vogler, 2006, p. 29). By virtue of the competences conferred upon, for example, the Commission, that entity can take some form of affirmative action in seeking to resolve policy or practical issues. In the case of cyber security, it can assign specific tasks to various agencies such as ENISA, Europol or eu-LISA.

This thesis proposes to merge Scharpf's postulation of "composite actors" with Bretherton and Vogler's conceptualisation and characterisation of "actorness". This new "Scharpf-Bretherton-Vogler" model of actorness can be applied to the formal institutions of the EU. By accepting the gestalt nature of the Commission, the Parliament, the European Council and the Council of the European Union these bodies can be considered as composite

actors, entities which speak with their own voice. In the field of cyber security these bodies have presence, opportunity and capability to act, thereby conferring upon them "actorness" under Bretherton and Vogler's definition.

The actors of relevance for this study are therefore the formal institutions of the EU. However, only four of the seven bodies which make up the modern EU are directly involved in the cyber security policy-making process: the European Commission, the European Council, the Council of the European Union and the European Parliament. The final three – the Court of Auditors, the Court of Justice and the European Central Bank – will not be examined in this thesis. The reason for this is that their purpose, function and tasks do not relate to the *development* of EU cyber security policy. While the Commission can refer Member States to the Court of Justice for failing to ensure ratification and implementation of legislation as per the Treaty regulations, the Court does not produce, determine or otherwise approve that legislation or make any policy decisions. The Court of Auditors is a body which exists solely to examine the financial actions of the other institutions while the ECB operates exclusively in financial and economic services. As such it may be a user of cyber security policy, but does not contribute to its developmental processes.

4.3.1.1. The Role of the Formal Institutions in EU Policy-making

Before embarking on an examination of the interaction of the relevant actors within an institutional setting, it is beneficial to set out their roles in the policy development process. The European Council sits at the apex of EU decision-making. It is comprised of the heads of state and government of the EU's Member States and, since the entry into force of the Treaty of Lisbon, is presided over by a permanent President. As of 1 December 2014, this is Donald Tusk, a former Prime Minister of Poland (European Council, 2014). This institution meets to discuss and steer the overall strategic direction of the Union as a whole, respond to major problems such as the 2008 economic crisis (Interview, Senior Official, DG MARKT, European Commission, 2014) and provide leadership for the EU at the highest political level (Dinan, 2010, p. 205). Despite having no legislative powers, its pronouncements – published as Conclusions and Resolutions – form the basis for subsequent strategy paths and policy development. Alongside the Treaties, these Resolutions establish and govern patterns of behaviour and procedural norms for the EU's constituent actors.

In line with the overall strategic direction set by the European Council, Union legislation is passed into law by two representative bodies – the Council of the European Union, and the European Parliament. The Council of the European Union is the institution representing Member State governments. It is where national, policy-specific ministers meet (European Council & Council of the European Union, 2014). Since the entry into force of the Treaty of Lisbon, the Council of the European Union shares legislative co-decision with the European Parliament. The Parliament is the only directly-elected EU body (European Parliament, n.d.). It represents the citizens of the Union. Its members do not sit in national blocs, but rather in larger groupings of Member State parties which share political ideology such as the European Peoples' Party[26] or the Socialists and Democrats[27].

The final institution involved in policy development is the European Commission (the Commission). Described as the engine room of EU policy and analogous to a national civil service (Robinson, 2012, p. 162) the Commission is responsible for the preparation, implementation and monitoring of EU policy and legislation and describes itself as the guardian of the Treaties (Interview, Senior Official, DG HOME, European Commission, 2014). It is divided into 28 departments called Directorates-General (DG). These are comparable to national ministries. They are each responsible for a policy portfolio and headed by a Commissioner. Commissioners are representatives from each of the EU Member States and are known collectively as the College of Commissioners. In the field of cyber security, the most relevant DGs are those responsible for Communications Networks, Content and Technology (DG Connect), Migration and Home (DG HOME) and Internal Market, Industry, Entrepreneurship and SMEs (DG GROWTH, formerly DG MARKT until the appointment of the Junker Commission in 2014). This thesis will therefore concentrate on the roles, actions and interactions of these four actors.

4.4. Path Dependence and Punctuation Points

In addition to specifying the actors and institutions to be examined, two further aspects of institutionalist analyses are significant for this thesis. These are path dependence and punctuated equilibrium. They are two closely related functions of historical institutionalism. These concepts stem from the notion that HI scholars "have a view of institutional development that emphasizes path dependence and unintended consequences" (Hall & Taylor, 1996, p. 938). The fundamental premise is that decisions made at the

[26] The EPP is comprised of centre-right, pro-EU Member State political parties (EPP, n.d.)
[27] Made up of left-wing national parties, such as the UK's Labour party and the German Sozialdemokratische Partei Deutschlands (S&D, n.d.).

commencement or at very early stages in a political or social process continue to have an influence on decisions made later on, until a critical juncture occurs to shift the path in a new direction.

4.4.1. Path dependence

Path dependence (PD) as a concept has been described in a number of ways. Pierson (2000, p. 251) argued that PD is predicated upon the premise that specific patterns of timing and sequence matter in socio-political analyses, and that small events can lead to large consequences. Thelen (1999, p. 385) describes PD as the process of "locking-in" policy choices as all relevant actors adjust their strategies to accommodate the prevailing pattern. Both of these conceptualisations imply a strong element of institutional "stickiness" (Pierson and Skocpol, 2002, p. 7). Once a choice is made it becomes difficult for actors to change those choices or deviate from the path embarked upon. This inertia occurs even when the resulting outcomes of those decisions are suboptimal or "manifestly inefficient" (Pollack, 2007, p. 3). It not only sets actors on particular policy paths, but excludes other choices and avenues for policy development (Bulmer, 1998, p. 367; Pierson, 1996). There is a caveat to using PD as an explanatory mechanism. Given the conceptualisations mentioned above, Mahoney (2000, p. 507) cautions against using PD to reduce the study of socio-political phenomena to mean "little more than the vague notion that history matters or that the past influences the future". Mahoney is criticising the potential for socio-political studies to be oversimplified and reduced to historical causality. This can be avoided by acknowledging that PD is a *function* of a wider institutionalist approach which examines the interaction of institutions and ideas, rather than a single explanatory mechanism on its own.

Path dependence is of particular relevance to this thesis. The object of this research is to understand what influence institutions have had on cyber security policy development and continuity. Answering this question from an HI perspective – i.e. over time – must involve an examination of, or at least an identification of, path dependent processes, in particular when examining policy continuity. The research undertaken to answer the thesis's questions will identify the extent to which cyber security policy choices made at the beginning of the timescape affected and effected choices or options at later stages.

A focus on PD also enables this thesis to apply one of the few specific methodological tools used in HI analyses. To identify path dependence Mahoney (2000, p. 507) argues that scholars must

> trace a given outcome back to a particular set of historical events, and show how these events are themselves contingent occurrences that cannot be explained on the basis of prior historical conditions.

As set out in Chapter 3, this technique was carried out in order to identify the commencement of EU interest in cyber security, thus establishing a timescape for the thesis.

4.4.2. Punctuated equilibrium

Although the institutional dynamic of path dependence is characterised by policy inertia and a resistance to change, there is a mechanism in HI scholarship by which policy paths can alter or be redefined. Once a path is embarked upon, a policy enters a period of consolidation or stasis. However, there are historical examples of major social and political crises necessitating changes in policy. Hall (1992, pp. 90–113) cites the example of the shift in UK economic policy from Keynesianism to monetarism in the 1970s. While there were institutional dynamics making policy-makers amenable to change, the catalysts for this shift were economic stagnation and rising inflation. Such catalytic events have the capacity to punctuate the equilibrium of established policy choices and amend or change the prevailing institutionalised options. This was the case in UK economic policy in the 1970s.

This mechanism is known as "punctuated equilibrium" (Krasner, 1984, p. 240). The central premise is that particular catalytic events occur which act as critical junctures or punctuation points in a policy path. They cause re-evaluations of past choices and enable previously locked-out policy options to be once again available. As Collier and Collier (1991, p. 29) argue, these critical junctures can cause either a temporary change in policy direction or "an extended period of reorientation". Thelen (1999, p. 385) goes a step further. She argues that the initial policy choice is itself a critical juncture and can cause a lock-in of subsequent paths. This is a similar conceptualisation to that of Lindner and Rittberger (2003, p. 448) who argue that the construction and creation of institutions is a phase distinct from their operation.

As will be examined in Chapters 8 and 9, in the case of EU cyber security policy, three such catalytic events occurred in the later years of the timescape. They put severe institutional stresses on the established socio-economic policy path. In 2007 Estonia suffered a series of cyber-attacks against its financial and e-government infrastructure. These attacks were allegedly state-sponsored and highlighted the EU's inability to act in

defence/military matters. In 2008 the global financial crisis highlighted the extent of network connectivity in international industry and financial sectors including those of the EU. This in turn formalised the consideration of cyberspace and ICT as a "critical infrastructure" for society. In 2009 the Treaty of Lisbon came into force, which radically altered the architecture of the EU and clarified its competences, paving the way for the EUCSS to be developed. This thesis will examine the effect of these catalytic events on the development of EU cyber security policy in order to identify whether they had any impact on that policy sector. This will provide an opportunity to assess the strength of path dependence in the context of EU cyber security.

4.5. Conclusion

This chapter clarified the institutions and actors relevant to this thesis and concludes the first, preparatory, section of the thesis. The chapter established certain core components necessary to carry out an effective HI analysis. The first of these are the institutions and actors to be researched. Following an empirical exercise involving analysing *acquis* and interview data, the institution on which this thesis will focus is Union competence. This defines not just the policy areas in which the EU can operate, but also the degree of involvement permitted. Certain policy sectors, such as military or national security, are red lines for Member States. As a result the Union has a very limited, highly regulated competence in these areas. In other areas such as the Eurozone and the customs union, the EU enjoys exclusive competence, where it acts as a supranational entity over and above the Member States. This thesis will examine the influence of competence on EU cyber security policy over the course of 28 years.

An HI analysis must also be clear on which actors are going to be the focus of the study. In addition to identifying the competences as the institution of greatest relevance to cyber security, the empirical exercise undertaken also identified which actors made policy decisions in this sector. Due to their policy-making remits these are the European Council, the European Commission, the Council of the European Union and the European Parliament. Also examined was the nature of these entities as actors. They are not unitary bodies, but represent the combined will of their constituents. These entities can however be considered actors with the application of a Scharpf-Bretherton-Vogler conceptualisation of "actorness". By combining Scharpf's definition of a composite actor with Bretherton and Vogler's three-part test of actorness – presence, opportunity and capability – the EU's formal institutions can be considered as actors operating within the institutional confines of

Union competences. This classification is important because it resolves the confusing issue of nomenclature by not referring to these entities as "formal institutions" in an institutionalist analysis.

The chapter has also examined certain facets of HI relevant to this thesis. Path dependence and punctuated equilibrium are two features common to HI analyses of the EU (Bulmer, 2009, 1998; Pierson, 1996; Pollack, 2006). The first examines the institutional forces which lead to policy continuity. The second goes some way to explaining policy change. Although these functions appear to be mutually exclusive, they are in fact complementary. As Bulmer (2009, p. 307) argues, path dependency and punctuated equilibrium are "dual dynamics". Particular choices, even small ones, can have long term consequences and lead to policy stasis and consolidation. However, major events such as external crises can punctuate that equilibrium and lead to a re-evaluation of policy choices. This has the potential to create new or divergent policy paths. Path dependence examines incremental development and punctuated equilibrium explains radical change. They are nevertheless two sides of the same coin. Political development, however incremental, is often "punctuated by critical moments or junctures that shape [it]" (Pierson, 2000, p. 251). Analysing this potential effect will form a core part of the following, empirical, chapters.

Chapter 5 | The EU's Cyber Security Discourse

5.1. Introduction

The EU's cyber security policy must be established before it can be analysed. This chapter will set out and clarify that policy. The chapter will provide evidence from analyses of the EU's *acquis communautaire* and elite interviews to argue that the EU has developed a specific socio-economic discourse focussing on resilience and co-operation.

A policy 'discourse' is the manner in which particular phenomena, policy issues or themes are framed and given meaning (Gasper and Apthorpe, 1996, p. 2). An analysis of 143 *acquis* documents collated for this thesis identified a socio-economic interpretation of risks and incidents originating in cyberspace. This infers a policy framework built around political, social and economic aspects of security. This sets it apart from the policies of other actors which have included national security or military considerations. Evidence from content analyses of EU *acquis* as well as analyses of interviews will be presented in this chapter to demonstrate that this idiosyncratic socio-economic discourse was constructed around five core ideational elements: maximising economic potential, building trust in digital networks, protecting fundamental rights, tackling cyber-crime and facilitating co-operation.

The chapter will make three arguments. It will show that the five core elements occur in Union *acquis* at all stages of the development of EU cyber security policy between 1985 and 2013. They first occur in the initial phase of development between 1985 and 2001. At that time they constituted important aspects of the establishment of the Single Market and attempts to develop information and communications technology (ICT) as a commercial sector. Once these policy paths were established, the five elements formed the kernel of the first formal attempts to create a cyber security policy, the *Commission Proposal for a Network and Information Security Strategy* of 2001 and the *Strategy for a Secure Information Society* of 2006. The second document was published at the end of a period of consolidation of policy goals. These five ideational elements would in turn form core aspects of the EUCSS published in 2013.

In addition to arguing that there exists an identifiable Union discourse in this policy sector, the chapter will demonstrate that that discourse continued unchanged throughout the 28-year timescape. While the cyber-threat landscape, and the security challenges emanating from cyberspace, evolved and changed between 1985 and 2013, the EU's basic discourse –

the manner in which it framed these phenomena – demonstrated an unusual element of continuity. While this chapter presents evidence of that continuity, subsequent chapters will explore the reasons behind it in order to answer the primary research question: *have institutions and institutional arrangements led the EU to develop and continue with a socio-economic approach to cyber security?*

Finally, the chapter will also present evidence that the discourse is not an *ad hoc* construct. By conducting historiographical analyses of both Union *acquis* and interview data, it will be shown that the discourse is the result of a long term developmental process which began in 1985. The combination of core ideational elements informed the development of policy and subsequent additions to the *acquis* throughout the 28-year timescape until the publication of the EUCSS of 2013.

The following section of the chapter sets out the EU's policy discourse. It examines in detail the EU's *Cyber Security Strategy*, the formal *acquis* document in which Union policy in this sector is set out. The section also introduces the five core ideational elements. Each element is then examined individually, to demonstrate ideational continuity throughout the policy development timescape. This is achieved by demonstrating the elements' presence in six *acquis* milestones in the EU's cyber security timescape. These milestones are:

- *1985 Commission Communication on Completing the Internal Market*
- *1994 Bangemann Report*
- *1996 Commission Communication on Illegal and Harmful Content*
- *2001 Commission Proposal for a Network and Information Security Strategy (NIS Proposal)*
- *2006 Strategy for a Secure Information Society (SSIS)*
- *2013 EUCSS*

5.2. The EU's cyber security discourse: An Historic Framework Based on Five Ideational Elements

On 7 February 2013 the Commission released the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (EUCSS) (European Commission, 2013a). This document sets out in detail the EU's cyber security policy. The Strategy itself is divided into four parts. The first section sets out the context and general principles for the Strategy, including ideational drivers which underpin the EU's cyber security response as a whole. The second part is the most developed section and examines five core strategic goals:

1. achieving cyber resilience;
2. drastically reducing cyber-crime;
3. developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
4. developing the industrial and technological resources for cyber security;
5. and establishing a coherent international cyberspace policy for the European Union to promote core EU values.

The section sets out how the EU intends to achieve these goals including naming key operational agencies – for example, ENISA and Europol – and assigning them specific tasks. These tasks include providing specialist analytical and operational support to Member States' cyber-crime investigations (European Commission, 2013a, p. 10) and

> assisting the Member States in developing strong national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure. (European Commission, 2013a, p. 7)

The third section of the EUCSS sets out the EU's view on the roles and responsibilities of various actors at national, EU and international level. It establishes how the Union will promote and facilitate channels for co-ordination and collaboration with these various bodies (European Commission, 2013a, p. 18). A fourth and final section concludes the Strategy by clarifying that the document is a joint effort between the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (HR). This makes the EUCSS the first joint project made possible by the changes to the structure of the EU brought in by the Treaty of Lisbon (European Commission, 2013a; Interview, Senior Official, EEAS, 2014)[28].

From a policy analysis perspective the most important part of the Strategy is Section 1.1 – the Context. That section sets out the ideational framework on which the Strategy itself is based. It presents the EU's interpretation of the inherent risks resulting from an increased use of ICT in every-day life. Every other facet of the Strategy, and the EU's cyber security response as a whole, is shaped by this interpretation.

The Context section is important for understanding the EU's cyber security policy because it is here that the EU departs from prevailing political narratives. A number of important actors treat cyber security as a national security matter. The US reserves the right to respond to cyber-incidents using "all necessary means", including military force (USA,

[28] See Chapter 9.

2011a, p. 14). In its National Strategy for Protection against Cyber Risks, Switzerland states that law enforcement agencies "are called to focus on cyber-attacks as severe offences relating to national security" (Switzerland, 2012, p. 30). Japan treats cyber-incidents which have a "crisis management" component in the same way as national security matters given their potential severity (Japan, 2013, p. 8). The Context section of the EUCSS, by contrast, places EU policy within a socio-economic, rather than national security or quasi–military narrative. Rather than concentrating on fighting or mitigating potential cyber-risks and threats, the EU focusses on the positive opportunities provided by ubiquitous wired technology. These opportunities can be used to protect fundamental rights and to promote economic growth. These goals are achieved by developing a discourse constructed upon five main themes, core norms, which run through all sections of the EUCSS. These elements are:

1. a concentration on maximising the economic potential of cyberspace,
2. creating citizen, corporate and political trust in new digital and online technologies,
3. protecting fundamental rights,
4. tackling cyber-crime
5. achieving these four goals through facilitating co-operation.

Although distinct concepts, these ideational elements operate together to inform the Union's discourse. While engendering trust in new technology and tackling online criminal activity were crucial to the economic viability of the internal market, so too was ensuring that EU citizens' rights to privacy were protected while online. The way that these four policy goals were to be achieved was through ensuring that all the actors co-operated with one another and shared relevant information. Just as the EU was ideally positioned to tackle online criminal activity, so too was it ideally positioned to act as a facilitator of this co-operation. It had the resources and capacity to act as a conduit for information and best practice between its Member States, the private sector and international partners.

The importance of these five elements is evidenced by their prevalence not just in the EUCSS, but throughout the *acquis.* The occurrence of these concepts is shown in Table 5-1 below. Out of 143 pieces of Union *acquis* studied for this thesis, the elements occurred a total of 548 times. The most frequent element was co-operation, which alone occurred 229 times, signifying the importance of this concept in EU cyber security policy.

Table 5-1: Ideational Elements in EU cyber security policy

Element	Economics	Trust	Rights	Cyber-Crime	Co-operation
Number of Occurrences	120	45	63	91	229

Having clarified the prevalence of these five ideational elements in Union *acquis*, and their significance in the EUCSS itself, the following sections of the chapter examine each concept in turn. These sections set out the concepts' influence on the EU's wider cyber security discourse.

5.2.1. Maximising the Economic Potential of Cyberspace

The EUCSS states that ICT has become the "backbone of [the EU's] economic growth and is a critical resource which all economic sectors rely on" (European Commission, 2013a, p. 2). The vital importance of ICT, and secure ICT infrastructures, to the economic growth and vitality of the Union is stressed in this phrase, and at every opportunity in the Strategy itself. Although ICT was crucial to protecting and promoting fundamental rights, the baseline ideological driver for the EU according to the EUCSS is the ability to utilise the economic and commercial opportunities presented by the exponential increase in ICT usage in all walks of life. Even the Union's focus on online criminal activity stems from a concern for the effect such activity has on the EU's economy as well as a strong concern for citizen welfare (European Commission, 2013a, p. 3).

Considering cyber security as a corollary to economic policy was, however, nothing new for the EU. The exercise of gathering Union *acquis* in this field demonstrated an interest in the ICT sector as far back as 1985. In a Commission Communication of that year on the establishment of the Single Market, the IT sector was considered to be one where economic growth and employment could be promoted (European Commission, 1985, p. 20). This interest continued over the next 28 years and into the EUCSS. Economic

maximisation was a concept important in all six *acquis* milestones in the policy-making timescape. This prevalence is shown in Table 5-2 below:

Table 5-2: Linear continuity of "economics" as an ideational element

1985 – Completing the Internal Market	1994 - Bangemann Report and 1996 - Illegal and harmful content	2001 – NIS Proposal	2006 – Strategy for a Secure Information Society	2013 - EUCSS
This general policy will put particular emphasis on certain sectors. These include information technology and telecommunications, construction and foodstuffs. In the information technology and telecommunications sector, the Commission wants to establish specific rules which take account of the requirement for much greater precision and more rapid decision-making so as to ensure compatibility, intercommunication and interworking between the users and operators throughout the Community. (European Commission, 1985, p. 20)	The information society has the potential to improve the quality of life of Europe's citizens, the efficiency of our social and economic organization and to reinforce cohesion. (Bangemann, 1994, p. 11) Driven by its meteoric growth, and its rapid evolution from· a government/academic network to a broad-based communication and trading platform, the Internet is currently revolutionising a number of economic sectors, with the emergence of a vibrant and fast growing "Internet Economy". Simultaneously, the Internet has also become a powerful influence in the social, educational and cultural fields (European Commission, 1996a, p. 3)	Security is becoming a key priority because communication and information have become a key factor in economic and societal development. Networks and information systems are now supporting services and carrying data to an extent inconceivable only a few years ago. Their availability is critical for other infrastructures such as water and electricity supply. (European Commission, 2001b, p. 1)	The relevance of the ICT sector for the European economy and for European society as a whole is incontestable. ICT is a critical component of innovation and is responsible for nearly 40% of productivity growth. In addition, this highly innovative sector is responsible for more than a quarter of the total European R&D effort and plays a key role in the creation of economic growth and jobs throughout the economy. More and more Europeans live in a truly information-based society where the use of ICTs has rapidly accelerated as a core function of human social and economic interaction. According to Eurostat, 89% of EU enterprises actively used the Internet in 2004 and around 50% of consumers had recently used the Internet (European Commission, 2006a, p. 5)	Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems. (European Commission, 2013a, p. 2)

As shown in Table 5-2, the initial EU interest in ICT came about as the result of a desire between 1985 and 1996 to extricate the EU from an economic recession. This is shown by the Commission earmarking ICT for particular attention alongside the construction and foodstuffs industries. This attention is particularly evident in ensuring EU-wide technological compatibility. By the mid-1990s economic benefits would be something all tiers of society could enjoy and not just the larger industrial economy.

By 2001, ICT was seen as a core component of the Single Market, as shown in the NIS proposal of 2001 (European Commission, 2001b, p. 1). The primary aim of that Proposal was to ensure the economic viability of information networks and infrastructures. It argued that security itself was a commodity bought and sold on the open market (European Commission, 2001b, p. 2). The NIS Proposal's rationale was to focus on data protection, securing a functioning economy, and protecting critical physical infrastructures. This combined the financial focus of the EU with Union security and ensured that "market imperfections" – gaps caused by security solutions not being considered profitable – were addressed (European Commission, 2001b, p. 2). Additional evidence of this importance can be found in the eEurope initiative of 1999 which was intended to help develop a knowledge-based economy (European Commission, 1999, 2001b, p. 4, 2000a, p. 2).

Building on policy choices made in the 1990s and early 2000s, by 2006 there was a clear understanding that an information society making full use of its opportunities meant that knowledge and innovation would be the "engines of sustainable growth" in European economies (European Commission, 2005, p. 3; European Council, 2003a, p. 14). This stemmed from a recognition that European society and the economy as a whole was becoming increasingly dependent on digital information (Council of The European Union, 2002b, p. 2). Small and medium sized enterprises (SMEs) could create jobs in the ICT sector (Council of The European Union, 2003, p. 1). A knowledge-based economy supported by efficient broadband internet networks would enhance competitiveness and growth (European Council, 2003b, p. 3). This was a core policy choice of the 2006 *Strategy for a Secure Information Society* (SSIS) which would continue into the EUCSS in 2013. As the "backbone" of EU economic growth (European Commission, 2013a, p. 2) a stable, uninterrupted internet was vital to large corporate interests as well as social sectors such as health and transport.

5.2.2. Promoting Trust in Digital Systems

According to the EUCSS a close corollary to ensuring the economic vitality of the Single Market and digital infrastructure is developing the trust that citizens and operators have in that infrastructure (European Commission, 2013a, p. 2,12). The logic behind this position was that, if individual citizens trust that their financial and personal data will remain secure when they are using the internet and cyberspace, then there will be an increase in online economic transactions such as commercial purchases and money transfers. A 2012 Eurobarometer survey found that a large proportion of internet users in Europe were not confident about their ability to use ICT for making online purchases or for banking (TNS Opinion & Social & European Commission, 2012, p. 68). The EU interpreted this as a lack of trust in the online commercial domain as a whole. A goal of the Strategy was to make the EU the safest online commercial space in the world.

The concept of "trust" as an ideational element also continued throughout the 28 year timescape. This is shown in Table 5-3 below.

Table 5-3: Linear continuity of "trust" as an ideational element

1994 – Bangemann Report; 1996 - illegal and harmful content	**2001 – NIS Proposal**	**2006 – SSIS**	**2013- EUCSS**
A great deal of effort must be put into securing widespread public acceptance and actual use of the new technology. (Bangemann, 1994, p. 12)	There is a risk that some users, alarmed by the many reports of security threats, simply choose to avoid e-commerce altogether. Others who are either uninformed or underestimate the risk may be too careless. Some companies may have an interest in underplaying potential risks, for fear of losing customers. (European Commission, 2001a, p. 20)	A breach in NIS can generate an impact that transcends the economic dimension. Indeed, there is a general concern that security problems may lead to user discouragement and lower take-up of ICT, whereas availability, reliability and security are a prerequisite for guaranteeing fundamental rights on-line. (European Commission, 2006a, p. 5)	For new connected technologies to take off, including e-payments, cloud computing or machine-to-machine communication, citizens will need trust and confidence. Unfortunately, a 2012 Eurobarometer survey showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases. An overwhelming majority also said they avoid disclosing personal information online because of security concerns. Across the EU, more than one in ten Internet users has already become victim of online fraud. (European Commission, 2013a, pp. 2–3)

Historically, trust in new digital systems came in a number of forms. In its earliest iterations in the Bangemann Report of 1996 it was simply the acceptance by EU citizens of new digital technologies and ways of doing business (Bangemann, 1994, p. 12). Citizen support for the new measures such as using digital technology to promote economic growth and create jobs was vital if the EU's new "information society" was going to take off and succeed (European Commission, 1994, p. 13). Building trust and confidence were primary objectives for promoting digital commerce (European Commission, 1997a, p. 13). By 2001, however, there was a concern that many citizen and commercial users would simply opt not to use e-commerce due to their perceptions of security threats (European Commission, 2001b, p. 20). Consumers and businesses had to be confident that their transactions would not be compromised and that identity data was secure. This focus on identity protection became a core component of EU policy, and was codified in legislation passed in 2004 (European Parliament & Council of The European Union, 2004, p. 3). Building on this legislative foundation, the 2006 SSIS was explicit in acknowledging the relationship between trust in digital networks and nascent cyber security. It stated that:

> A breach in NIS can generate an impact that transcends the economic dimension. Indeed, there is a general concern that security problems may lead to user discouragement and lower take-up of ICT (European Commission, 2006a, p. 5).

Trust was considered crucial to cyber security and this consideration continued into the EUCSS. For new technologies such as cloud computing and machine-to-machine communications, EU citizens "will need trust and confidence" (European Commission, 2013a, p. 2).

One way to ensure, or at least promote, this trust was through ensuring that citizen privacy was protected online. According to both the 2006 SSIS and the 2013 EUCSS, therefore, trust was of particular pertinence to another core ideational element of the EU's discourse: "guaranteeing fundamental rights online" (European Commission, 2006a, p. 5).

5.2.3. Protecting Fundamental Rights

One of the key tools used to build trust in the online domain was the protection of fundamental rights, particularly the right to personal privacy. As stated in the EUCSS, cyber security itself can only be sound and effective if

> it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally,

> individuals' rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field (European Commission, 2013a, p. 4).

According to Clemente (Interview, Clemente, Chatham House, 2014), the logic behind this was, if citizens are protected from online fraud and if their privacy and personal data is secure, they will be encouraged to use the internet and cyberspace for business and social transactions. This will in turn promote economic growth.

Of the 148 references to the protection of fundamental rights made in Union *acquis* over the course of the 28 year timescape there are 60 references to the right to privacy alone. This includes the issue being cited as one of the central principles underpinning EU cyber security policy (European Commission, 2013a, p. 4). In the early stages of policy development, privacy was a concern for users of new digital technologies. It was of such concern that a regulatory framework to ensure privacy was proposed in 1993 (European Commission, 1993, p. 24). In a rare move in this policy sector, legislation in the form of a *Directive on electronic communications networks* was passed (European Parliament and Council of the European Union, 2002a, p. 42). This demonstrated the EU's commitment to this policy goal.

Personal privacy as a fundamental right to be protected therefore has a longstanding presence throughout the EU's cyber security policy-making timescape. This was recognised by the EU in a 1992 reference to Article 8 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms* (European Commission, 1992a, p. 7). Such protection was vital to the functioning of the information society (European Commission, 1995, p. 85, 2000b, p. 9,12). It made no difference to the protection of privacy that personal information was being stored in digital formats.

The policy goal of protecting fundamental rights extended beyond ensuring data protection and personal privacy. One of the key principles for cyber security established by the EUCSS is "access for all" (European Commission, 2013a, p. 4). Digital illiteracy or a lack of access to the internet for individuals and businesses meant that citizens may be disadvantaged in an economic sense. They would not have access to the same economic opportunities as wired individuals or businesses. In addition, the unhindered flow of information translated into an avenue for freedom of expression and the exercise of fundamental rights. The EUCSS cites the use of ICT and the internet as mouthpieces for

protesters in the Arab Spring (European Commission, 2013a, p. 2) as an example of the effectiveness of wired technology in this regard.

Just as privacy was not a new concept for the EU, neither was ensuring access to the internet and its opportunities. Between 1985 and 2013 this access was recognised as a fundamental right in and of itself. It included the right to access new technology and to gain digital literacy (Bangemann, 1994, p. 11; European Council, 2001, p. 22). According to the Council of the European Union, a lack of access should not hinder the uptake of social and economic opportunities (Council of The European Union, 1997, p. 4). What changed by the time the EUCSS was published was the explicit recognition of this right to access as a core component of cyber security policy (European Commission, 2013a, p. 16). The internet and cyberspace were considered as tools not just for commercial and economic opportunities, but for promoting social justice.

Such an ideological standpoint represents a departure by the EU from the prevailing cyber security narrative, particularly when considering government surveillance. The EUCSS explicitly warned against government misuse of cyberspace for surveillance of and control over their own citizens (European Commission, 2013a, p. 3). This caution extended into the private sector with warnings against the mass collection of data by major corporations (Reding, 2012) and the right for citizens to have data removed from online searches under the so-called "right to be forgotten" (Bennett, 2012, p. 162). The focus for EU cyber security is not just the supranational concept of the economic viability of the internal digital space. That focus takes account of the individual citizens who use that space. This is reflected in the underlying purpose of critical infrastructure protection (CIP). The importance of protecting critical infrastructures from cyber incidents is included in the EUCSS (European Commission, 2013a, p. 7,16). The *purpose* of that protection, however, is to ensure usability and trust for the end-user rather than using such concepts as an excuse to invade privacy with heavy-handed surveillance (Deibert, 2009, p. 327). Over time, the EU has positioned itself in the cyber discourse not just as a champion of fundamental rights and freedoms but as a check on overzealous government monitoring.

The enduring focus of the EU on privacy is shown in the excerpts cited in Table 5-4 below. As with the previous ideational elements, these excerpts are taken from specific *acquis* milestones published between 1985 and 2013:

Table 5-4: Linear continuity of "protection of fundamental rights" as an ideational element

1994 – Bangemann Report; 1996 - illegal and harmful content	2001 – NIS Proposal	2006 – SSIS	2013 - EUCSS
Certain issues do not involve protection of public order, but rather the protection of the rights of individuals (protection of privacy and reputation) and of an environment allowing creation of content to flourish (intellectual property). (European Commission, 1996a, p. 10)	Protection of privacy is a key policy objective in the European Union. It was recognised as a basic right under Article 8 of the European Convention on human rights. Articles 7 and 8 of the Charter of Fundamental Rights of the European Union also provide the right to respect for family and private life, home and communications and personal data. (European Commission, 2001a, p. 24)	A breach in NIS can generate an impact that transcends the economic dimension. Indeed, there is a general concern that security problems may lead to user discouragement and lower take-up of ICT, whereas availability, reliability and security are a prerequisite for guaranteeing fundamental rights on-line. (European Commission, 2006a, p. 5)	Support the promotion and protection of fundamental rights, including access to information and freedom of expression, focusing on: a) developing new public guidelines on freedom of expression online and offline; b) monitoring the export of products or services that might be used for censorship or mass surveillance online; c) developing measures and tools to expand Internet access, openness and resilience to address censorship or mass surveillance by communication technology; d) empowering stakeholders to use communication technology to promote fundamental rights. (European Commission, 2013a, p. 16)

5.2.4. Tackling Cyber-Crime

A prominent method used to protect fundamental rights and promote trust was to tackle the problem of data theft and privacy breaches. This was done by tackling computer-related criminal activity known as cyber-crime. As early as 1996 the EU recognised such activity as one of the fastest growing forms of crime (European Commission, 1996a, p. 3). According to the EUCSS, such criminal acts were transnational (i.e. were conducted irrespective of national borders) and caused a variety of social and economic problems. These ranged from privacy breaches and the online exploitation of children (European Commission, 2013a, p. 9) to stealing critical proprietary data or holding companies to ransom (European Commission, 2013a, p. 3).

By 2013 the EU's interpretation of cyber-crime extended beyond criminal activity for personal or corporate gain to include economic espionage and state-sponsored activity (European Commission, 2013a, p. 3). This is important as it is another departure from the prevailing academic and political narrative. National actors such as Japan and the US cite these as latent national security threats (Japan, 2013; USA, 2011b, p. 40). Academic

scholarship examining such issues tends to place these activities within a national security, "cyber warfare" analytical framework (Farwell and Rohozinski, 2011; Lindsay, 2013; Lischka, 2013).

The EU by contrast considers these issues as threats to the economic viability of cyberspace. This interpretation positions these state-sponsored activities firmly within a socio-economic discourse. The EU's response to the cyber-attack on Estonia in 2007 was to treat it as a criminal threat to the ongoing functionality of the internal market[29]. Although the scale of the incident was acknowledged (European Commission, 2010b, p. 2) along with its technical sophistication (European Commission, 2009a, p. 4), at no point does the EU use militaristic language such as "cyber war" to describe it. Instead the incident was interpreted as one which could have an adverse effect on commercial and citizen use of the internet and the digital domain in much the same manner as other forms of "economic" cyber-crime. Even espionage is categorised by the EU as an economic threat in the EUCSS (European Commission, 2013a, p. 3). This provides further evidence of an underlying discourse in EU cyber security policy. If the standard approach to cyber security issues is to treat these as socio-economic threats, then *any* incident would be treated as a criminal act. This includes those with alleged state involvement.

As shown in the comparison table 5-5 below, throughout the 28-year timescape the EU was not blind to the fact that there are those seeking to take advantage of the openness and accessibility of cyberspace for criminal or state gains (European Commission, 2001a, 1996a).

[29] The Estonian cyber-attack of 2007 is examined in greater detail in Chapter 8 Section 2 of this thesis.

Table 5-5: Linear continuity of "tackling cyber-crime" as an ideational element

1994 – Bangemann Report; 1996 - illegal and harmful content	2001 – NIS Proposal	2006 – SSIS	2013 - EUCSS
Reflecting these opportunities, the vast majority of Internet content is for purposes of information for totally legitimate (and often highly productive) business or private usage: However, like any other communication technologies, particularly in the initial stages of their development, the Internet carries an amount of potentially harmful or illegal contents or can be misused as a vehicle for criminal activities. (European Commission, 1996a, p. 3)	The proposed policy measures with regard to network and information security have to be seen not only in the context of the existing telecommunications and data protection legislation but also in relation to the more recent cyber-crime policies. The Commission has recently published a Communication on cyber-crime which foresees, amongst other initiatives, the setting up of an EU Forum on cybercrime with the aim of enhancing mutual understanding and co-operation at EU level between all interested parties. (European Commission, 2001a, p. 19)	Making proposals for improving co-operation between law enforcement authorities and addressing new forms of criminal activity that exploit the Internet and undermine the operation of critical infrastructures. This will be the subject of a specific Communication on cybercrime. (European Commission, 2006a, p. 6)	The EU economy is already affected by cybercrime activities against the private sector and individuals. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies. (European Commission, 2013a, p. 3)

As early as 1994, fewer than 10 years after the EU expressed interest in ICT, it was recognised that digital data and content could be used for illegal or harmful purposes. Any medium of information exchange could be exploited for criminal gain (European Commission, 1996a, p. 3). Throughout the EU's cyber security historiography, however, all references to such activity refer to it as criminal. Network and information security breaches (European Commission, 2001a, p. 19), exploitation of weaknesses in critical infrastructure (European Commission, 2006a, p. 6) and "state-sponsored activity" (European Commission, 2013a, p. 3) are all acts to be responded to by law-enforcement agencies, and not state security apparatus.

Rather than play into the prevailing, negative, national security-focussed narrative the EU maintained the position that cyberspace offers huge opportunities for commerce, private sector innovation and social freedoms. As stated in the EUCSS, cyberspace "breaks down barriers between countries, communities and citizens, allowing interaction and sharing of

information and ideas across the globe" (European Commission, 2013a, p. 2). There is no mention in the EUCSS of cyber war or cyber warfare. All security threats to, and emanating from cyberspace, were classified as socio-economic risks, further highlighting the nature of the EU's underlying policy narrative or discourse in this field.

5.2.5. Co-operation as a *modus operandi*

According to the EUCSS, the central methodological approach of the EU to achieving its conceptual goals is facilitating co-operation. Cyberspace is a borderless domain and cyber-risks and threats have a cross-border dimension (European Commission, 2013a, p. 9). The EU institutions and bodies are ideally placed to facilitate the development of a co-ordinated and collaborative approach to mitigating these risks (Interview, Smith and Jones, eu-LISA, 2014). That includes bringing the private sector into formal joint-working protocols such as the European Public-Private Partnership for Resilience (EP3R) (European Commission, 2013a, p. 6) or co-ordinating international cyber security exercises between nation states (European Commission, 2013a, p. 7; Interview, Purser, ENISA, 2014).

The reason for this focus on co-ordination in the EUCSS was a recognition that such work on the part of the EU should not be carried out at the expense of Member State initiatives, or in lieu of Member State capabilities. The EU sought to "bring together law enforcement and judicial authorities and public and private stakeholders from the EU and beyond" (European Commission, 2013a, p. 10). The aim was to complement rather than supersede the work of the Member States. This also enabled the EU to maintain its adherence to subsidiarity.

This is exemplified by the fact that the EU engaged in an arms'-length approach to achieving security predicated upon encouraging and incentivising the private sector and national agencies. In the 2006 *Strategy for a Secure Information Society* (SSIS) the EU established itself as a facilitative actor. Its function was not to prescribe specific solutions or recommend specific technical measures (Interview, Purser, ENISA, 2014). This reflected a longer-term trend of seeking to *develop* co-operation between actors throughout the cyber security policy-making timescape, as shown in Table 5-6 below.

Table 5-6: Linear continuity of “co-operation” as an ideational element

1994 – Bangemann Report; 1996 - illegal and harmful content	2001 – NIS Proposal	2006 – SSIS	2013 - EUCSS
Even if a published document is removed from one server as a result of intervention by the authorities, it can easily and quickly be copied to other servers in other jurisdictions, · so that it continues to be available unless and until such sites are also blocked. Thus additional international co-operation is required to avoid "safe havens" for documents contrary to general rules of criminal law. (European Commission, 1996a, p. 12)	Co-operation is essential to ensure early warning throughout the Union through the instantaneous exchange of information on the first signs of attack in one country. Therefore co-operation with the CERT system within the European Union should be strengthened as a matter of urgency. A first action aiming at strengthening the public/private co-operation on dependability of information infrastructures (including the development of early warning systems) and improving co-operation amongst CERTS has been agreed in the context of the eEurope action plan. (European Commission, 2001a, p. 21)	The global dimension of network and information security challenges the Commission, both at international level and in co-ordination with Member States, to increase its efforts to promote global co-operation on NIS, notably in implementing the agenda adopted at the World Summit on the Information Society (WSIS) in November 2005. (European Commission, 2006a, p. 7)	To promote cyber resilience in the EU, both public authorities and the private sector must develop capabilities and co-operate effectively. Building on the positive results achieved via the activities carried out to date further EU action can help in particular to counter cyber risks and threats having a cross-border dimension, and contribute to a co-ordinated response in emergency situations. (European Commission, 2013a, p. 5)

The rationale was that if all actors co-operated and co-ordinated their efforts, cyber security would be closer to being realised (European Commission, 2013b, p. 8,9). The purpose the EU was giving itself between 1985 and 2013 was to facilitate that co-operation. This is because it is acknowledged that no single actor can achieve cyber security on its own (European Commission, 2010b, p. 3, 2013a, p. 17; European Parliament and Council of The European Union, 2011, p. 6). Co-operation, information-sharing, on-going dialogue, co-ordinated regional, national and international measures are the fundamental aims of the EUCSS. The Strategy tasked agencies such as ENISA and Europol with pursuing those aims (European Commission, 2013a, p. 10).

The concept of co-operation also defined what kind of cyber security actor the EU was seeking to be. Due to restricted competences and an explicit acknowledgement that

responsibility for achieving cyber security remained with the Member States, the EU set itself up as a facilitative actor. It was to be a lynchpin in international efforts designed to tackle transnational cyber risks. This is a role which the EU has the capacity, resources and crucially the competence to play[30]. It has set up specialist agencies tasked with operationalising certain aspects of co-operation and co-ordination in specific policy areas. The European Defence Agency (EDA) and the European External Action Service (EEAS) facilitate co-ordination and co-operation in foreign and defence policy. The European Network and Information Security Agency (ENISA) assists Member States with ensuring the resilience of infrastructures vital to the internal market and Europol, through the European Cyber-Crime Centre (EC3), co-ordinates vast amounts of data and law enforcement resources in tackling online criminal activity. On a conceptual basis, co-operation was therefore a core element of the EU's entire approach to tackling cyber security threats and risks, and continued to be so throughout the 28 year timescape of policy development.

5.3. Conclusion

This chapter has shown that the EU developed a specific approach to cyber security as a policy sector over the 28 years between 1985 and 2013. That approach – its discourse – was focussed on treating the field as a socio-economic issue. Cyber security challenges, including criminal activity, breaches of privacy and even state-sponsored acts of aggression, were treated as threats to the ongoing functionality of the internal market. From the time the internal market was initiated, ICT and the burgeoning Internet were seen as vital sectors for the EU which could be used to promote economic growth and employment. Cyberspace and cyber security were crucial for the ongoing economic wellbeing of the Union. The EU's unique position as a transnational actor meant that it was ideally positioned to tackle such issues as cyber-crime, with a view to promoting private citizen and commercial trust in new technologies. The EUCSS, representing the sum total and culmination of a policy-making process, is the exemplar of this discourse. Its initial chapters – in which the context for all EU cyber security policy in 2013 is set out – are founded upon that socio-economic discourse.

The chapter also included a comparative analysis of the EUCSS with its conceptual predecessors. The results of this analysis demonstrate that it was not a stand-alone

[30] See Chapter 4 Section 3.1 on "actorness".

document. It was the culmination of a long-term process of applying a discourse constructed around five core ideational elements created at the initiation of the EU's interest in ICT in 1985. These elements are: maximising economic potential; promoting trust; protecting fundamental rights; tackling cyber-crime and achieving these through fostering co-operation. These elements persisted in an unaltered manner throughout the EU's timescape in this policy sector. In the 143 pieces of Union *acquis* identified for this thesis, these five ideational elements are the most frequently occurring concepts, underpinning the EU's cyber security policy narrative. They are paths from which the EU did not deviate throughout the 28 years of the policy-making process and underpin the EU's socio-economic discourse.

The EUCSS is therefore not just a part of a policy discourse, but the result of a cumulative, linear, evolutionary progression. By comparing key elements, namely five ideas underpinning a socio-economic policy, this chapter has demonstrated that linearity. By tracing the policy-making process through its various iterations in 1996, 2001 and 2006 the chapter has shown that the policy discourse was static. In the 28 years between 1985 and 2013 the threat landscape may have changed and new tools developed to address those threats, but the EU's underlying discourse did not change. It remained focussed on the socio-economic priorities key to EU policy.

While not inferring a deterministic policy-making progression, the continued presence of these ideational aspects represents the strongest element of path dependency in EU cyber security policy and policy-making. The strength of this path dependency will be demonstrated in subsequent chapters of this thesis, when the resilience of the discourse to institutional stresses is examined.

The next task of this thesis is to examine how this path dependent discourse came about and look at *why* the EU's discourse remained static. As stated in Chapter 1, a supplementary question for this thesis is whether or not the institutional influence of Union competences – the rules and standard procedures regulating policy-making – created an environment in which only socio-economic solutions could develop. The following chapters will examine the empirical data gathered to answer this question. This will address a key aspect of the substantive research question of this thesis by identifying an institutional arrangement which contributed to policy continuity in cyber security.

Chapter 6 | Creating Path Dependence 1985-2001

6.1. Introduction

The previous chapter set out the European Union's discourse in cyber security. It demonstrated that ideas established in the 1980s, at the earliest points of the policy development process, continued to affect subsequent decisions and the framing of the EU's discourse until 2013. The aim of this chapter is to build on this discussion of the EU's discourse by explaining how those path dependencies were established. This is important because the aim of the thesis is not simply to identify which institutions and institutional arrangements affected cyber security policy. By focussing on the period between 1985 and 2001, the chapter also seeks to examine how and why those arrangements led to the development of the EU's idiosyncratic, socio-economic cyber security discourse and influenced its continuity.

The choices which established path dependence in EU cyber security policy can be traced back to four important events which occurred early in this sector's timescape. These events are the establishment of the Single Market, the publication of the Bangemann Report, the signing of the Single European Act and the entry into force of the Maastricht Treaty. Each of these events established particular institutional dynamics which affected the later development of cyber security policy.

This chapter will first examine the how the initiation of the Single Market in 1985 affected cyber security policy. This event was one of the most important milestones in the history of the EU itself. As an economic program it was intended to extricate the EU from the deep recession of the 1980s by any and all means available. ICT and the developing Internet were viewed by the EU as areas of great social and commercial opportunity, economic growth and employment. Small and medium-sized enterprises (SMEs) in this sector were to be supported and encouraged to grow in order to boost employment within a single, internal market for goods and services. This focus on the developing cyber domain as a place of commercial opportunity initiated a core ideational element of the EU's cyber security discourse: economic maximisation. That maximisation was initiated by the publication in 1994 of the Bangemann Report. This was one of the most important documents in the EU's cyber security policy timescape, as it contained the conceptual seeds for all elements of the EU's discourse and "cyber" policy.

At the same time as the importance of ICT for the nascent Single Market was being established, a parallel process was occurring which further entrenched this socio-economic focus: the Treaty-based codification of Union competences. This chapter will examine the effect of the restriction of Union competences in security matters, formalised in the Single European Act and the Maastricht Treaty, on EU cyber security policy. As a consequence of the provisions of the Treaty of Maastricht and the Single European Act, EU action and capacity in security matters – its competences – were restricted to "political and economic aspects" (European Union, 1987, p. 1049). While not considered controversial or problematic at the time, this restriction had far-reaching consequences for the future development of cyber security policy. The lack of Union competence in "hard" security issues would place cyber security considerations on a path of non-military, socio-economic policy development.

This section of the chapter will also examine the importance of timing: the EU's competences influenced the extent to which the EU could become involved in a security matter, cyber security. However, those competences were solidified and codified *after* the commencement of the EU's interest in ICT as a social and commercial sector. This is an important element of an HI analysis as it marks the point where path dependencies were established in cyber security. Although Union interest in ICT and its concomitant security issues began *before* the EU started to codify its competences, once those competences were in place the earlier interest in cyber security could not be expanded. Its socio-economic focus was locked in place.

The argument will be made in this chapter that the combination of a conscious interest in ICT as a tool for economic growth coupled with restricted Union competences in security matters created a socio-economic path dependency in cyber security. As a result of restricted competences and the positioning of ICT policy in the Internal Market area, security risks and issues such as increased online criminal activity, data or identity protection issues and copyright infringement were treated as threats to the functionality of the nascent internal market and citizen wellbeing. In other words they were treated as socio-economic issues. When examining potential security and safety risks, there was little mention of national security or military issues. This socio-economic focus of cyber security coalesced by 2001 into a Commission proposal for a network and information security strategy. This proposal, the first document representing an identifiable cyber

security policy in the EU, codified the socio-economic preferences of the Union in this policy sector, further entrenching the nature of the EU's discourse in this field.

The chapter is divided into six sections. Following this introduction, the second section examines the establishment of identifiable "cyber" policies in the context of the initiation of the Single Market. The third section explores the formalisation of Union security competences, examining the important fact that this formalisation occurred *after* the commencement of the EU's cyber security discourse, but had a significant influence on that discourse's subsequent development. The fourth section of the chapter examines the EU's responses to nascent cyber security concerns during this period. The fifth section examines the EU's first formal attempt to develop a recognisable cyber security strategy, a document entitled *Network and Information Security: Proposal for a European Policy Approach,* published in 2001. The sixth section concludes the chapter.

6.2. Establishing Union "cyber" policy

6.2.1. The Initiation of the Single Market and the Focus on ICT

As set out in Chapter 5, the EU's cyber security discourse is predicated upon five core ideational elements: maximisation of economic opportunities, establishing trust in systems and networks, protecting fundamental rights, tackling cyber-crime and achieving these through promoting and facilitating co-operation. The chronological and historiographical development of this discourse inferred a linear, but not deterministic progression from a concentration on the commercial opportunities of digital technology in the mid-1980s to the publication of the EUCSS in 2013.

The exercise undertaken to establish the timescape of policy development (described in Chapter 3) also established that the conceptual germ for EU cyber security policy can be found in the initiation of the Single Market Programme (SMP). Begun in 1985 (Bulmer, 1998, p. 365), the SMP was the EU's strategy for building a common, unified market for European goods and services, as well as facilitating the movement of those goods (European Commission, 1985, p. 6). In the early 1980s Europe as a whole was mired in an economic recession (Young, 2010, p. 111). While the economies of the USA and Japan were improving thanks to markets in consumer electronics and defence, Europe was falling behind (European Commission, 1993, p. 9; Staab, 2013, p. 93). The thinking was that an internal market would greatly increase economic growth across the membership of the Union. Citizens would have a wider choice of products and services, originating not just in

their home country but other Member States. Capital would move freely from one national banking sector to another and citizens would have the right to live and work anywhere in the EU (Staab, 2013, p. 92). This would not only generate wealth but create jobs. The EU was therefore seeking any and all avenues to reverse the downward economic trend and tackle unemployment. The SMP was the centre-piece of Union policy designed to achieve these goals.

To advance this project, on 14 June 1985 the European Commission under Jacques Delors presented to the European Council a White Paper entitled *Completing the Internal Market* (European Commission, 1985). This Communication is one of the most important documents produced by the Commission (Dinan, 2010, p. 79). It positioned that actor as the "institutional entrepreneur" of the SMP (Fligstein and Mara-Drita, 1996, p. 11). In addition to setting out why the EU should establish a single economic area, the White Paper also defended market liberalisation as a means to stimulate growth across the Union membership. In its most ambitious chapters, it also set out a timetable for the creation and implementation of the Single Market (Dinan, 2010, p. 79; European Commission, 1985, p. 57). Although a massive project which would radically alter the economic and political face of Europe, the Commission envisaged its establishment by 1992 (European Commission, 1985, p. 62).

Due to its significance in setting up core concepts such as the free movement of goods, services and people, the White Paper was a milestone in the evolution and development of the EU as a whole. It was also the first step in the process that would lead to the development of the EU's unified response to cyber security challenges, the EUCSS of 2013. In its 1985 Communication the Commission identified a number of sectors where EU action could potentially be beneficial. As well as telecommunications and foodstuffs, information technology (IT) was singled out for specific attention (European Commission, 1985, p. 20). As part of the construction of the internal market, a service industry based around IT – a relatively new sector at the time – would be encouraged.

IT and the Single Market therefore complemented one another. It was recognised that sectors such as audio-visual industries, information and data processing and computerised marketing and distribution could only achieve their potential within a "large unobstructed market" (European Commission, 1985, p. 30), i.e. a single marketplace where goods and services could move freely. The ultimate aim of the Single Market as regards IT was to

reduce, and prevent the creation of, obstacles to innovation and economic growth inherent in a fragmented market (European Commission, 1985, p. 6). Creating a permissive, facilitative environment where burgeoning industries and sectors such as IT could develop would in turn facilitate wealth and job creation, economic growth and promote the functioning of the internal market once it was launched.

The IT sector was seen as an untapped domain of commercial opportunity. This conceptualisation represented the initiation of a core element of the EU's interest in this sector: using new digital and information technologies to promote economic growth by exploiting the potential of this new domain[31]. Demonstrating a remarkable degree of prescience, it was argued that, with the right regulatory framework, the digital domain could become a flourishing economic space in its own right (European Commission, 1985). An unobstructed single market with reduced controls and a permissive environment, created through the removal of internal boundaries, customs protocols and the establishment of free movement of goods and services would support this digital domain. This would in turn enable SMEs to capture the full potential of digital media to stimulate growth and create jobs.

The importance of stimulating employment as a goal for the EU in this period was further cemented in 1993 by another White Paper from the Commission entitled *Growth, Competitiveness and Employment: The Challenges*. This White Paper was produced at the behest of the European Council (European Council, 1993a, p. 7). Its self-professed "one and only reason" (European Commission, 1993, p. 9) for publication was to counter unemployment. This was a core motivation for EU economic policy at the time, a goal to be achieved through addressing weaknesses in Member State national economies. Although nine million jobs had been created since 1985, more needed to be done to stimulate industry in a measured way without a "dash for economic freedom" causing further damage to the nascent recovery (European Commission, 1993, pp. 9–10).

What makes this White Paper of relevance and importance to the future development of a Union cyber security policy is that a core element of this medium-term strategy was the

[31] The importance of ICT to economic growth would be repeated in the EUCSS. "Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems." (European Commission, 2013a, p. 2).

recognition of the need for ever greater and swifter development of new information technologies (European Commission, 1993, p. 15; European Council, 1993b, p. 9). Two "development themes" were promulgated by the Commission in this second White Paper. As was the case in 1985, specific economic sectors were listed where EU attention should focus. One was trans-European transport and energy networks (European Commission, 1993, p. 28). The second was information networks (European Commission, 1993, p. 22).

Recognising an increase in the use of electronic multimedia in social and commercial life, the EU sought to build on its previous promotion of that sector by developing a digital version of the single market. Information highways would be constructed with the same goals as international motorways: to enable the free, unfettered flow of information to support international commercial enterprises (European Commission, 1993, p. 14, 1995, p. 12,21). The idea was to develop a European digital space, an idea representing another step in the incremental development of EU cyber, and hence cyber security, policy.

This digital domain was a cornerstone of EU economic and social development for a number of reasons. Not only would European economies benefit from an increased communicative and co-operative capability afforded by developments in IT and other forms of digital media, but the EU itself was ideally placed to act as a facilitator of that communication and co-operation (European Commission, 1993, p. 65). This facilitative role would become a key feature of later EU cyber security policy. The EU's *Cyber Security Strategy* (EUCSS) of 2013 proposed that the EU act as a facilitator of security. It aimed to ensure the spread of knowledge and best practice, as well as bringing actors together rather than legislate or stipulate specific technological solutions (European Commission, 2013a, p. 18; Christou, 2016).

Once ICT and a digital domain had been posited as a beneficial tool for economic and social development by the Commission, the European Council noted the benefits these brought to the manner in which European economies were managed and maintained. As stated in the European Council's conclusions of December 1993:

> The new information and communication technologies…have brought about fundamental changes in the structures and methods of production. Europe must adapt itself quickly to these developments and must control their consequences. Those economies which are the first to complete this transformation will have a significant competitive edge. (European Council, 1993b, p. 11).

Due to this acknowledgment, and in additional recognition of the influence of information and communications technologies (ICT) on European society as a whole, the European Council tasked the Commission to report on specific measures to develop and implement a European digital space. The result was another milestone in EU cyber security policy-making: the Bangemann Report of 1994.

6.2.2. The 1994 Bangemann Report

The Bangemann Report was one of the most important documents in the foundation and development of EU cyber security policy. The reason for this is that the origins of all the core elements in that policy discourse can be traced back to this document. While the initiation of interest in ICT can be found in the White Paper establishing the Internal Market in 1985 (European Commission, 1985), it was in the Bangemann Report that this interest began to coalesce into a more recognisable "cyber" policy.

The Bangemann Report was specifically requested by the European Council in a meeting in Brussels in 1993 (European Council, 1993b, p. 11). The Commission was tasked with sponsoring and co-ordinating a committee of experts who would examine the fundamental social and economic changes brought about by emergent ICT. At the time it was recognised that Europe as a whole had to adapt to these new technologies as "those economies which are the first to complete this transformation [to ICT] will have a significant competitive edge" (European Council, 1993b, p. 11). Once again economic factors were the primary driving force for this measure. To ensure this economic competitive advantage, the European Council therefore requested:

> that a report be prepared for its next meeting by a group of prominent persons fully representative of all relevant industries in the Union and of users and consumers, designated by the Council and the Commission, on the specific measures to be taken into consideration by the Community and the Member States in this sphere (European Council, 1993b, p. 12).

The report was to cover the development and interoperability of infrastructure networks "for facilitating the dissemination of information" as well as basic trans-European services such as databases and email (European Council, 1993b, p. 12).

The purpose of the Bangemann Report was to examine the economic and social implications and potential of digital infrastructures and new media. However, it inadvertently established certain policy choices which became standard goals and aims for

all cyber policies produced since. This included those documents dealing with security and safety issues. In effect, the Report created crucial path dependencies in this particular field (Fligstein and Mara-Drita, 1996, p. 5). This linear connection between the Bangemann Report and the EUCSS can be demonstrated with a tabular comparison of key elements of both documents.

Table 6-1: Comparison of the Bangemann Report and the EUCSS[32]

Bangemann Report 1994 (Bangemann, 1994)	***European Cyber Security Strategy 2013*** (European Commission, 2013a)
Economic factors including market forces	Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on.
Data protection and online privacy must be enshrined rights	**Protecting fundamental rights, freedom of expression, personal data and privacy** Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field.
Creation of Jobs	The EU should make the best of the Horizon 2020 Framework Programme for Research and Innovation, to be launched in 2014. (Horizon 2020 is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness. Running from 2014 to 2020, the EU's new Framework Programme for research and innovation will be part of the drive to create new growth and jobs in Europe).
Intellectual property and online piracy must be combatted	Across the EU, more than one in ten Internet users has already become victim of online fraud.
EU (particularly Commission) must promote actor co-operation	The Commission and High Representative will increase policy co-ordination and information sharing through the international Critical Information Infrastructure Protection networks such as the Meridian network, co-operation among NIS competent authorities and others.
Private sector involvement crucial	Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth.

[32] In this table, general references to the document source have been placed in the column heading, rather than for each individual point. This was done for ease of reading.

As shown in Table 7 above, the Bangemann Report and the EUCSS share certain vital components, indicating a direct connection between the concepts initiated in 1994 and those published in the EUCSS of 2013. The Bangemann Report makes clear that economic factors such as market forces (Bangemann, 1994, p. 16) and the creation of jobs (Bangemann, 1994, p. 10) underpin the Union's interest and strategic outlook in ICT. This position is a cornerstone of the EUCSS as it is acknowledged that cyberspace "has become the backbone of our economic growth and is a critical resource which all economic sectors rely on" (European Commission, 2013a, p. 2; Interview, Smith and Jones, eu-LISA, 2014). In 1994, data protection and online privacy were fundamental rights to be enshrined both in the information society and in future policy (European Commission, 1996c, p. 12). These are to be ensured via technical and regulatory measures (Bangemann, 1994, p. 22,131).

The protection of fundamental rights such as privacy and safety, online or offline, are core tenets of the EUCSS (European Commission, 2013a, p. 4). Dr Udo Helmbrecht, the Executive Director of ENISA, stated that basic civil rights cannot be ensured without data protection (Interview, Helmbrecht, ENISA, 2014). This view is echoed by officials from eu-LISA (Interview, Smith and Jones, eu-LISA, 2014). The precursors to the regulatory framework for intellectual property rights and combatting online piracy were also established in 1994 (Bangemann, 1994, p. 21). This would form a core element of tackling cyber-crime by 2013 (European Commission, 2013a, p. 9) including the establishment of the European Cyber Crime Centre at Europol (Europol, 2013a).

The linear connection is not restricted simply to policy aims or strategic goals, however. The Bangemann Report also states that the way these goals would be achieved was for the EU, in particular the Commission, to facilitate actor co-operation, particularly the pooling of resources (Bangemann, 1994, p. 12). This view is echoed by the Commission facilitating the sharing of information and best practice amongst core interested parties under the terms of the EUCSS (European Commission, 2013a, p. 16). There was also in 1994 a growing recognition of the importance of the private sector in this regard (European Council, 1994a). An entire chapter of the Bangemann Report is devoted to securing private finance and ensuring that the private sector accept responsibility and take a lead role in the development of future initiatives (Bangemann, 1994, p. 34). The role of the private sector in EU cyber policy does not diminish over the next 28 years. In 1996 the private sector was seen as crucial for developing Internet and multimedia use in education

(European Commission, 1996d, p. 16), and by 2013 it was a lynchpin in securing the EU's digital space (European Commission, 2013a, p. 2,5).

Core path dependencies in cyber security policy were established when the Bangemann Report was endorsed by the European Council (European Council, 1994b, pp. 7–8). A strong economic focus was instituted, centring on employment and economic growth. As established in Chapter 5 of this thesis on the EU's discourse, Union cyber security policy acknowledges that ICT infrastructures form the backbone of economic and social life. The choices made in the Bangemann Report focussed policy attention on socio-economic factors such as wealth creation and employment. This in turn would lead to the adoption of a more socio-economic approach to the manner in which the EU would seek to secure its digital space. The aim was for the EU to become a digital domain in which to do business with confidence, in safety and with access to numerous new commercial opportunities.

In 1994 these policy choices sought to maximise the potential for new technologies and ICT to contribute to the economic and social development of the EU (European Council, 1994b, p. 8). This policy was part of the wider international movement towards digital and online media in that it set in train a crucial policy choice – a path dependence – which ultimately would differentiate it from other cyber security strategies of the 2010s. As examined in Chapter 1, the EU takes a very different approach to cyber security to most other actors. A number of key cyber security actors take a more active position against external intrusions (Dewar, 2014, p. 14) or "attacks" under the laws of armed conflict (Dinstein, 2012, p. 264). Although a legitimate policy choice, it is one predicated upon a pessimistic view of cyberspace as a domain replete with myriad threats, threat agents and potential disasters which may occur leading to concentrations on worst-case scenarios (Dunn Cavelty, 2012a, p. 22) .

The EU in 2013 takes a more optimistic view. It seeks to establish a digital space where people can live, interact, communicate and do business safely and securely, confident in the knowledge that their data is safe and the infrastructures they are using are resilient (European Commission, 2013a, p. 2, 1994, p. 5). This positive position was established in the Bangemann Report and persisted for the next two decades. The developing digital space, what would eventually be labelled as "cyberspace", was seen not as a realm of danger, but as one of great commercial opportunity for European society to enjoy and

exploit (European Commission, 1996b, p. 2, 1994, p. 3). Exploited opportunities needed to be safe and secure, but this did not detract from the EU's positive attitude to cyberspace and digital media, an attitude which persists in the EUCSS with its description of "an open and free cyberspace" (European Commission, 2013a, p. 2). According to officials at eu-LISA, the fundamental purpose of the EU's involvement as a body in digital and online technology is to promote a free, open and secure internet (Interview, Smith and Jones, eu-LISA, 2014).

The initiation of the Single Market and the publication of the Bangemann Report established a number of vital path dependencies for EU cyber security policy which would both affect and effect policy choices in later decades. A focus on maximising growth and employment cemented the economic prioritisation of EU policy as regards cyberspace as a whole. A consequence of this was that the EU considered cyberspace as a domain filled with opportunities, rather than threats, a view which was perpetuated throughout the timescape of cyber security policy development.

However, at the same time as socio-economic paths were being laid down a clarification of the EU's capacity to act in core policy sectors was also occurring. Against the backdrop of the establishment of the Single Market, the EU's competences were being codified, in particular those relating to security and external policy. While the Single Market and the Bangemann Report would create strong path dependencies in cyber security policy with respect to its economic foci, highly specified competence in security matters would have an equally important influence on the ability of the EU to respond to the security issues that arose along with the increased social and commercial use of ICT and the internet.

6.3. The Influence of Competence on Establishing Cyber Security Principles

6.3.1. The 1987 Single European Act

In the years between 1985 and 2001, the period in which EU cyber security policy foundations were established, two important Treaties entered into force which had a direct impact on all areas of policy-making, including cyber security: the Single European Act of 1987 and the Maastricht Treaty of 1992.

In September 1985, two months after the Commission published its landmark White Paper on completing the Internal Market (European Commission, 1985), a move commenced to

re-evaluate and reform the Treaties governing the functioning of the European Communities. Amidst acrimonious debates in the European Council, an intergovernmental conference (IGC) began (Dinan, 2010, p. 80). Buoyed by the relative success of the Single Market, negotiations progressed towards a radical reshaping of the Communities system through a Single European Act (SEA).

One of the most important elements of the SEA was that for the first time a treaty base for European political co-operation (EPC) was set out (Smith, 2015, p. 287). This established measures for future co-operation across the whole range of Union activities and moved the EU away from intergovernmentalism (Staab, 2013, p. 18). The SEA also mentioned the concept of "security" for the first time in this EPC framework. What is of particular consequence for cyber security policy-making is that it restricted the EU to "political and economic aspects" of security (European Union, 1987, p. 1049). In 1987 this softer approach to security was of greater symbolic significance than of practical importance. In its infancy as the European Coal and Steel Community the EU's purpose was to facilitate the development of an international system which veered away from military conflict. It did this by promoting economic, social and political co-operation (Dinan, 2010, pp. 17–18). To have this enshrined in a treaty seemed logical. This restriction was codified in the Petersberg Tasks of 1992 which specified that any military action under an EU banner would be restricted to peace-making, peacekeeping and rescue tasks (EEAS, n.d.). The SEA and Petersberg Tasks were, however, of crucial significance for *future* attempts to address security problems, in particular those which arose from cyberspace.

The SEA's restriction of European involvement in security and foreign policy issues to their political and economic aspects drastically reduced the EU's capacity to develop a truly holistic approach to cyber security. The scale of interconnectedness of the Internet, as well as the number of critical infrastructures which would rely on a functioning cyberspace by 2013, was a problem unforeseen in 1987. To borrow a phrase from chaos theory, the drop in the ocean that was the logical restriction of the EU to non-military, non-defence security considerations would create serious ripples (Gleick, 1997) when it was recognised by the 2000s that these areas were intricately linked due to the nature of cyberspace.

Because this issue was not foreseen, the EU continued on its softer security path post-SEA. By 1992 the restriction to socio-economic aspects of security was further entrenched by the

signing and entry into force of the Treaty on European Union, better known as the Maastricht Treaty. While the SEA established the parameters for security policy, the Maastricht Treaty set up a policy-making framework which would further curtail the EU's capacity to develop policy in foreign and security matters. It placed this sector in an intergovernmental policy-making and legislative process. This would require unanimous decision-making in the Council of the European Union. By contrast, economic decisions could be passed by a qualified majority. This divided system would become known as the Pillar System of the EU.

6.3.2. The 1992 Maastricht Treaty and the creation of policy pillars

It is not the aim of this section of the chapter to enter into a lengthy analysis of the terms of the Maastricht Treaty. Such analyses have been conducted elsewhere (Bache et al., 2011; Bulmer, 1997; Dinan, 2010). However it is beneficial to briefly consider the terms of the Treaty and how it affected Union policy- and decision-making in general before examining its precise impact on cyber security policy paths.

While the SEA established a co-operative framework for EU policy, the Maastricht Treaty was the first major revision of the Union's structure, policy-making processes and organisation since the 1957 Treaty of Rome. At its heart were measures to introduce elements of political union (Europa, n.d.). In addition to tools for co-operation, the Treaty initiated specific measures to promote greater political and economic integration. These included preparations for economic and monetary union (Dinan, 2010, p. 82; Staab, 2013, pp. 19–21) and the creation of a "European Union" founded on the European Communities (European Union, 1992, p. 7). Core aims of the Treaty were the completion of the Internal Market project begun in 1985 (European Union, 1992, p. 4) predicated upon the free movement of goods, services, persons and capital (European Union, 1992, p. 12). One of the most important aspects of the Treaty was the establishment of jurisdictions of responsibilities between the Member States and the EU: the areas of "competence" for each party.

For the EU, these competences were designed to set out in which areas the Union could create legislation and policy. As examined in Chapter 4, under this system, there were certain areas of "exclusive competence", where the EU had sole jurisdiction. Under the principle of subsidiarity, it made more sense for the supranational entity that was the EU to

draft policy or legislation than for the individual Member States to do so due to the nature or scale of the policy area (European Union, 1992, p. 13; Interview, Purser, ENISA, 2014).

One level down from exclusive competence was shared competence, where decision-making would be carried out by both the EU *and* the Member States. The majority of areas of Union policy would fall under this heading and incorporate the policy- and decision-making processes of the Treaty of Rome. Decisions in these policy areas would be taken via the "Community Method", whereby votes in the Council of the European Union were passed by a qualified majority (QMV). The functioning of the Internal Market and other aspects of economic policy fell into this category, including the nascent field of cyber policy. This comprised the first "pillar" of the new European Union.

The European Commission was afforded a right of initiative in this area, whereby it could propose policy and legislation if it saw a need (without instruction from the Council of the European Union or the Parliament). These proposals were subject to final decisions being made by the Council.

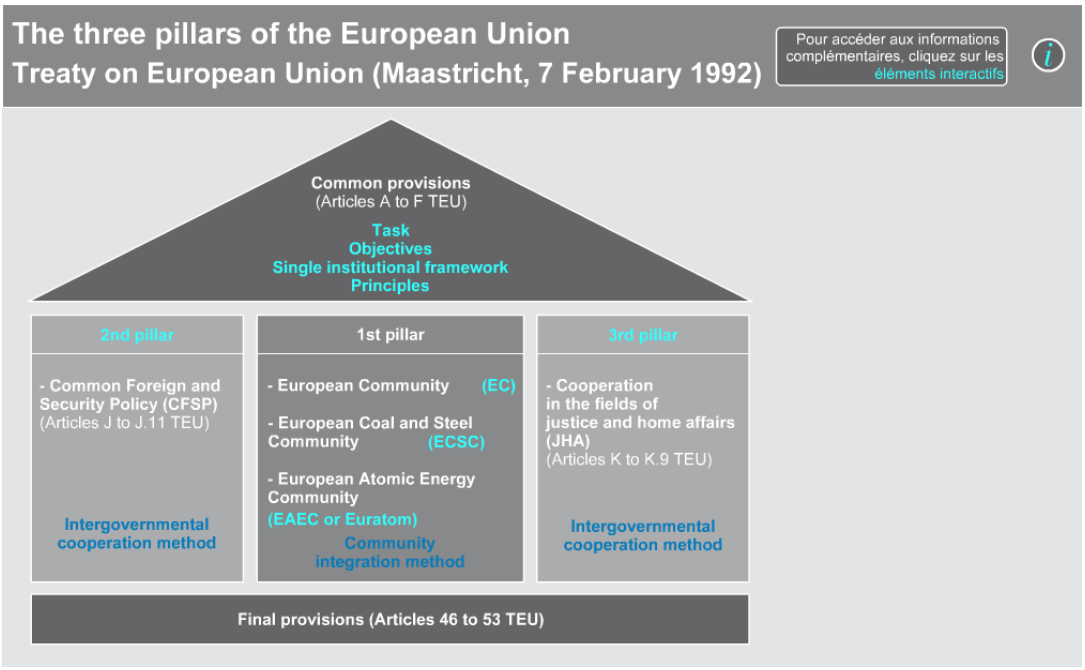
The Treaty also established two other fields of policy-making. These were the areas of the Common Foreign and Security Policy (CFSP)[33], and co-operation in the fields of Justice and Home Affairs (JHA). The key difference in these areas was the method of decision-making. Rather than using QMV, unanimous intergovernmental decisions were required.

The result of this division of remits was a system of three specific areas of Union policy, defined by their decision-making setup. These became known as the "Pillars of the EU", illustrated in the diagram below[34].

[33] The Common Foreign and Security Policy pillar was established despite the EU having very limited external competence (See Chapter 4). The aim of the CFSP was to enable the EU to speak on the international stage with one voice (European Union, 2016). Although military competence is highly restricted, in the field of diplomacy and international partnership, the EU speaking as a single entity has more "clout" than were each individual Member State to engage in its own.

[34] Image Source
http://www.cvce.eu/en/obj/the_three_pillars_of_the_european_union_maastricht_7_february_1992-en-37b4b8c8-0f00-4c1c-bec8-bcdf4b26807d.html

Diagram 6-1: The Pillars of the EU post Maastricht



As stated above, the Internal Market fell into the First Pillar, the Communities. Due to their importance to the Internal Market, ICT (cyber) issues also came under this policy- and decision-making system. This enabled the EU to engage proactively with those issues in an economic sense due to its shared competence. Union cyber security policy contains at its core a strong economic focus. The origins of this economic focus have been shown to be traceable to the initiation of the internal market in 1985 (European Commission, 1985, p. 20), and to subsequent moves to establish a secure information society (Bangemann, 1994; European Commission, 1996a, p. 96). The Treaty of Maastricht served to solidify this approach by placing cyber issues within a decision-making Pillar, the bulk of which concentrated on the functioning of the internal market.

Placing cyber policy within this First Pillar had another consequence, however, particularly since criminal justice matters were handled under the Third Pillar of JHA. It further restricted the manner in which the EU could address security issues emanating from cyberspace. The reduced security competence enshrined in the SEA and the codification of foreign and security policy into the intergovernmental CFSP Pillar therefore restricted EU cyber security policy to socio-economic matters. It is significant, however, that this

institutional restriction was put in place *after* the EU's socio-economic interest in ICT was established. What that restriction did was prevent any deviation from already established paths and lock out other potential avenues of cyber security policy or solutions outside of the socio-economic discourse.

This does not mean that the EU was naïve in its perception of the developing digital domain, or its own information society (European Commission, 1996e, p. 5). As the 1990s progressed, the EU became increasingly aware of the capacity for cyberspace and the internet to be abused (European Commission, 1996a). However, the placing of criminal justice policy in a separate Pillar to the Internal Market complicated the capacity of the EU to respond to this abuse. It necessitated a creative approach on the part of the Union to such issues in order to be able to effectively address them and ensure the viability of the Single Market. That approach would be to interpret online criminal activities as threats to the ongoing functionality of the Single Market, thus making them socio-economic issues.

6.4. Responding to Increasing Security Concerns

The initiation of the Single Market in 1985 and the Bangemann Report of 1994 were crucial milestones in the development of EU cyber security policy because they established the Union's economic focus in this sector. The provisions of the SEA and the Treaty of Maastricht were similarly important as they codified the capacity of the EU to engage in security matters.

While the EU was keen to exploit the economic, social and political opportunities of new digital media, the path to that exploitation was not without issue. The chronology of EU cyber security *acquis* demonstrates that, by 1996, concern was emerging that the Internet was being used to transmit harmful or illegal material – such as extreme pornography or content inciting racial hatred – as well as being "misused as a vehicle for criminal activity" (European Commission, 1996a, p. 3). This established a conceptual basis for the need for some sort of security policy addressing citizen and business interaction over the Internet. This set the stage for more specific network and information security (NIS) policies in the future.

The combined effects of these two paths can be seen in the Commission's 1996 Communication entitled *Illegal and Harmful Content on the Internet* (European Commission, 1996a). This was another milestone in the development of cyber security

policy as it established the core security components of what would become the EUCSS *within* the socio-economic framework established by its antecedents. Chief amongst these components was a list of security concerns set out in the Communication's introduction. The Commission cited these threats and risks as having the potential for direct repercussions on the functioning of the Internal Market[35] (European Commission, 1996a, p. 3). They are significant contributions to the cyber security policy timescape and hence merit citing here in full (emphasis in original):

- *national security* (instructions on bomb-making, illegal drug production, terrorist activities);
- *protection of minors* (abusive forms of marketing, violence, pornography);
- *protection of human dignity* (incitement to racial hatred or racial discrimination);
- *economic security* (fraud, instructions on pirating credit cards);
- *information security* (malicious hacking);
- *protection of privacy* (unauthorised communication of personal data, electronic harassment);
- *protection of reputation* (libel, unlawful comparative advertising);
- *intellectual property* (unauthorised distribution of copyrighted works, e.g. software or music)

The list of security threats is significant for two reasons. The first is that it retained the socio-economic prioritisation placed on ICT resulting from that sector's importance to the Single Market (European Council, 1993a, p. 26) and formalised in the Bangemann Report. Protection of copyright, fraud prevention, illegal advertising and abusive marketing are predominantly economic concerns as they could affect user confidence in the EU's digital space (European Commission, 1996a, p. 16). Data privacy and the protection of minors (European Commission, 1996a, p. 3) are predominantly social concerns, focusing on citizen safety and wellbeing.

The second reason this list is significant is perhaps more pertinent to the evolution of a recognisable "cyber security" policy. Issues such as the dissemination of bomb-making instructions, terrorist activities, protection of personal privacy, the incitement to racial hatred[36] and electronic harassment[37] were specifically cited as security and safety issues. A comparative exercise examining the content of the EUCSS and the Commission's

[35] This further reinforces the economic approach of the EU to this field.
[36] Comparable to Conway's (2005) conceptualisation of extremist propaganda as "cyber-cortical warfare".
[37] More colloquially known by 2015 as "trolling" (Hardaker, 2010; Herring et al., 2002).

Communication on Illegal and Harmful Content (an exercise similar to that carried out between the EUCSS and the Bangemann Report in the previous section) demonstrates the similarity and linear progression evident between the two documents. This comparison is shown in Table 6-2 below.

Table 6-2: Comparison of the EUCSS and COM (1996) 487

COM (1996) 487 (European Commission, 1996a)	***European Cyber Security Strategy 2013*** (European Commission, 2013a)
national security (instructions on bomb-making, illegal drug production, terrorist activities); *protection of minors* (abusive forms of marketing, violence, pornography);	Cybersecurity efforts in the EU also involve the cyber defence dimension. To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyber defence capability development should concentrate on detection, response and recovery from sophisticated cyber threats.
protection of human dignity (incitement to racial hatred or racial discrimination);	Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred). The EU international engagement in cyber issues will be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights.
economic security (fraud, instructions on pirating credit cards);	Across the EU, more than one in ten Internet users has already become victim of online fraud.
information security (malicious hacking);	Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies
protection of privacy (unauthorised communication of personal data, electronic harassment);	**Protecting fundamental rights, freedom of expression, personal data and privacy.** Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field.
protection of reputation (libel, unlawful comparative advertising);	
intellectual property (unauthorised distribution of copyrighted works, e.g. software or music)	Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), [and] content-related offences.

The only category which does not continue directly from 1996 to 2013 is that of *protection of reputation*. That being said, the specific subheading under the 1996 category includes libel and unlawful comparative advertising. It can be inferred that the modern phenomenon of "trolling" – publishing negative, deliberately damaging or hurtful comments on social media – could conceivably fall into both the 1996 category as being damaging to reputations and the 2013 category of protecting human dignity and rights[38].

In the same way that there is a demonstrable linear progression from the economic policies of the Bangemann Report to the EUCSS, there is also such a linear progression from the Commission's *Communication on Illegal and Harmful Content* to the EUCSS. When combined with the path dependencies established in 1994, this demonstrates that the EU's *cyber Security Strategy* was a product of policy decisions made in the 1990s.

This continuity or linearity is further demonstrated by the enduring nature of the security challenges faced. Security concerns regarding the exponential increase in the use of ICT by private citizens and commercial enterprises had up until this point been focussed on the protection of "natural persons" when their data was being processed via digital technologies (European Council, 1992, p. 29). To ensure adequate protections, and to engender trust in the new digital infrastructure, in 1992 the Commission issued proposals for two Directives which addressed issues which would become more widely known as "data protection". One related to the protection of computer databases (European Commission, 1992a) and the other related to citizens' personal and private information contained in those databases (European Commission, 1992b).

The objective of these Directives was to address the disparity of legal protection across Union membership and to recognise that unauthorised access to such databases could have "the gravest economic and technical consequences" (European Commission, 1992a, p. 1). There was an acknowledgment that some form of coherence and harmonisation of efforts across the Member States in the field of digital information protection would improve citizen and corporate trust in new media as well as facilitate the development of the internal market as a whole (European Parliament & Council of The European Union, 1995, p. 31, 1996, p. 20). This demonstrated that the focus for the EU at this point was not on the physical infrastructure underpinning cyberspace, but on digital information.

[38] The protection of human dignity and minors in audio-visual and information services was itself the subject of a separate Commission Green Paper published in the same year, demonstrating the importance placed by the EU on this particular sub-field (European Commission, 1996f).

In a rare move in the field of cyber security policy, legislation was passed between 1995 and 1997 to protect personal data, databases and personal privacy (European Parliament & Council of The European Union, 1995, 1996, 1997)[39]. The move towards legislation began in 1991 when it was recognised that computer programmes necessary for networked communication were not sufficiently protected by current legislation in all Member States. Such legislation that did exist was not standardised (Council of the European Union, 1991, p. 1). The same was true of computer databases where citizen and corporate information was being stored (European Parliament & Council of The European Union, 1996, p. 1). The primary purpose of this legislation, therefore, was to introduce that missing coherence by bringing all Member States up to a certain minimum level of legal protection for both databases and the software on which those databases ran. Coherence and harmonisation would later become core elements of EU cyber security policy and action (Interview, Purser, ENISA, 2014).

In addition equivalency of protection would be achieved across the Union Membership, particularly for personal and private citizen data (European Parliament & Council of The European Union, 1995, p. 32). This was to be achieved by all Member States being required to "bring into force the laws, regulations and administrative provisions" (Council of the European Union, 1991, p. 7) required in order to ensure compliance. The appetite for legislation continued with the passing in 1997 of the *Data Protection Directive*. That Directive sought to achieve:

> the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community (European Parliament & Council of The European Union, 1997, p. 4).

The ultimate goal of this legislation, however, was to facilitate the free movement of data within the Union while at the same time ensuring a high level of protection for individuals

[39] While it was, and still is, unusual for the EU to pass formal legislation on cyber issues, it is important to note that the legislation passed in this first Phase were Directives. In the typology of EU legislative instruments – Regulations, Directives and Decisions (European Union, n.d.) – a Directive is "a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals." (European Union, n.d.). Directives therefore establish a framework or set of goals to be achieved, but Member States are left to their own devices when implementing or establishing measures designed to achieve those goals.

with regard to the processing of their personal data and ensuring the development of open telecommunications networks.

It is apparent that the EU was at this point beginning to engage in the facilitative role identified by commentators in Chapter 2 (Christou, 2016). It was flexing its muscles and enjoying the confidence boost of the successful initiation of the Single Market. Passing legislation on a specific aspect of that Market was symptomatic of this increased confidence. The backdrop to these specific measures to increase harmonisation and equivalency however, was twofold. On the one hand was the requirement to carry out these measures for the smooth functioning of the new Single Market (European Parliament and Council of The European Union, 1996, p. 20, 1995, p. 31; European Commission, 2000b, p. 17). On the other, there was a growing realisation that the new technologies being advocated had the capacity to transmit potentially harmful content, make the dissemination of illegal material easier and for the technology itself to be misused by criminal elements. While the benefits of the exponential growth of the Internet and its content far outweighed any potential drawbacks, the effects of illegal and harmful content could not be ignored (European Commission, 1997b, p. 1). To address this, the EU developed an action plan for promoting the safe use of the Internet designed to establish a common approach to the threats posed by illegal and harmful online content, as well as to draw together the disparate instruments used in that approach.

An obstacle to achieving this facilitative role became apparent at this point. By the late 1990s, the EU's approach to cyber security consisted of a large collection of *acquis communautaire* of varying types. There was an array of regulations, policies, Council Conclusions and other *acquis* instruments which addressed issues ranging from personal privacy (EEA Joint Parliamentary Committee, 1994; European Parliament and Council of The European Union, 1995) to unauthorised access to the communications of the European Commission. There was, however, no unifying strategy covering security issues in cyberspace.

Seeing the need to ensure citizen and commercial trust and confidence in an increasingly interconnected society and information-driven economy, the European Council, under the presidency of Sweden, resolved in 2001 to work with the Commission to develop a "comprehensive strategy on the security of electronic networks including practical implementing action" (European Council, 2001, p. 23). ICT was becoming increasingly

important to economic growth, competitiveness and the development of a more inclusive society (European Commission, 2000b, p. 2; European Council, 2001). In addition, digital technology was becoming increasingly important to the functioning of critical national infrastructures (European Commission, 2001a, p. 7). Securing these would be achieved through international co-operation (European Commission, 1998, p. 4).

The result of this convergence of recognition was the first formal attempt to produce a unified EU policy dealing with cyber security; a document entitled *Network and Information Security: Proposal for a European Policy Approach* published by the European Commission in 2001 (European Commission, 2001a).

6.5. Creating a Recognisable "cyber security" policy: The 2001 *Proposal for a Network and Information Security Strategy*

The 2001 Proposal was a crucial milestone in cyber security policy-making for four reasons. First, it laid out a detailed typology of threats from cyberspace. Second, it recommended specific technical measures to improve security. Third, it provided a definition of NIS that would persist in EU policy in this sector until 2013, and finally, it formalised the placing of actor co-operation front and centre in the developing cyber security discourse.

6.5.1. Defining a Threat Typology

To cement its cyber security credentials and demonstrate that it was engaging with emerging digital threats, the EU's Proposal laid out a specific threat typology comprising six areas of risk:

1. Interception of communications;
2. Unauthorised access into (sic) computers and computer networks;
3. Disruption of the Internet and telephone networks;
4. Execution of malicious software that modifies or destroys data;
5. Malicious misrepresentation;
6. Environmental and unintentional events (European Commission, 2001a, p. 5)

The purpose behind providing these definitions was to give a comprehensive breakdown of the types of risks faced by national and private operators as well as bring coherence to the

list of risks published in 1996 (European Commission, 1996a, p. 3). What makes this typology important to the development of cyber security policy, and different to the list provided in 1996, is that the new typology for the first time acknowledged specific harmful *actions* taken against the digital infrastructure itself rather than just harmful content. Previous descriptions of risks and threats had focussed on the impact of harmful and illegal data, such as child pornography, or actions which utilised networked technology such as fraud and piracy. Although malicious hacking was considered a threat in 1996 under the "information security" heading, by 2001 the digital infrastructure itself had become a referent object of security policy, to the extent that disruption of the Internet itself was considered a significant risk (European Commission, 2001a, p. 12). This point in the timescape marks the commencement in EU policy making of recognising the Internet and ICT networks as critical infrastructures in their own right.

6.5.2. Specifying Technical Measures for Network and Information Security

To supplement the codified and streamlined threat typology, the NIS Proposal set out a series of specific measures designed to increase cyber security. The Proposal actively promoted (*inter alia*) the use of encryption in communications, not just by private citizens, but also communications corporations (European Commission, 2001a, p. 10). Also specified was that anti-virus software should be used to combat unauthorised access to digital systems (European Commission, 2001a, p. 12) and that domain name system (DNS) protocols should be extended to ensure that networks were not disrupted (European Commission, 2001a, p. 13).

These recommendations are unusual in their specificity. The EU had not until this point issued definitive practical guidance on combatting illegal or harmful content or unauthorised access to systems. Instead it sought to raise awareness of these potential risks, so that interested parties could make their own choices regarding solutions. The 2001 Proposal was a hands-on approach to NIS which demonstrated an increase in confidence on the part of the EU. It felt itself in a position to state what action should be taken by interested parties to combat NIS problems and hence actively engage in a security issue it considers important.

6.5.3. Defining Network and Information Security

To demonstrate Union confidence in cyber security, the 2001 Proposal issued a definition of network and information security (NIS) for the first time in Union policy. This definition would be the cornerstone of EU policy in this field for the subsequent twelve years. Predicated upon ensuring the confidentiality, integrity, authentication and availability of data (European Commission, 2001a, p. 9), NIS was defined as:

> the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems (European Commission, 2001a, p. 9).

Providing this definition had the effect of bringing a level of clarity, consistency and commonality of understanding to EU policy in this field and set the tone for future attempts to revise or revivify interest in this area. Cornish (2009, p. 9) and Klimburg & Tiirmaa-Klaar (2011, p. 11) have argued that European cyber security policy at the time suffered from a lack of cohesion, a high level of fragmentation and duplication amongst competing legislation, strategy initiatives and agencies. The definition of NIS provided by the 2001 Proposal was an attempt to address that fragmentation and lack of cohesion by providing formal working definitions of core concepts.

6.5.4. Promoting Actor Co-operation

The most prominent measure for ensuring security and minimising risks in the 2001 Proposal – and a core component of the EU's cyber security discourse – was actor co-operation. In 2001 this co-operation was manifested in sharing best practice (European Commission, 2001a, p. 21). One of the most important elements in developing resilient systems to protect critical infrastructures was for the actors involved in service provision and maintenance – the private network operators and national authorities – to exchange information on threats as they occurred. It was noted that experienced engineers were surprised by the novelty of some incidents. This highlighted the need for a reliable warning system and framework for information-sharing across the EU (European Commission, 2001a, p. 21). It was further noted that Computer Emergency Response Teams (CERTs) had been established in some Member States by 2001. Belgium was specifically mentioned (European Commission, 2001a, p. 21). However, it was also noted

that co-operation between these CERTS was problematic due to differing operational parameters and levels of expertise.

The Commission therefore proposed to develop measures to strengthen co-operation and facilitate information exchange. It also intended to examine, in co-operation with Member States, "how to best organise at European level data collection, analysis and planning of forward-looking responses to existing and emerging security threats" (European Commission, 2001a, p. 22). This was of particular importance for tackling online crime. In a foreshadowing of the establishment of a high-tech crime centre at Europol the following year, the 2001 Proposal envisaged the establishment of an EU forum on cyber-crime to "enhance mutual understanding and co-operation between all interested parties" (European Commission, 2001a, p. 19). The sharing of information and best practice would be vital tools in the fight against cyber-crime, and the EU with its inherent internationality, was ideally placed to facilitate this.

The NIS Proposal was an important step in EU cyber security policy-making because of these policy choices. It was the first recognisable "cyber security" policy. While previous *acquis* documents had addressed the core aspects of cyber security and initiated important policy paths, the NIS Proposal was the first time these had been brought together. The sum total of all of these actions was that the 2001 NIS Proposal drew together the elements which established the path dependencies of EU cyber security policy-making in subsequent years. The ultimate aim of EU policy in the period between 1985 and 2001 was the protection of economic viability and capabilities. This was to be achieved through ensuring that the systems and networks which underpinned this economic viability were able to continue functioning and providing the services for which they were designed (European Commission, 2001a, p. 3). To achieve this, the NIS Proposal defined exactly what NIS was, clarified the threats involved and provided a clear policy framework in order to address those threats. In 2001 this framework was based on harmonising private sector protocols, the sharing of information on security breaches, ensuring the continuity of critical services and an explicit commitment to treat malicious incidents as criminal acts.

6.6. Conclusion

This chapter has shown that important cyber security policy paths were established between 1985 and 2001. In 1985 the Single Market was established with a focus on ICT as an industry for investment and economic growth. In 1987 the Single European Act entered

into force, followed by the Maastricht Treaty in 1992. These two Treaties established the EU's competences in economic affairs and restricted its capacity in external security and defence policy. Together, these three milestones created a socio-economic environment in which future cyber security policy would develop. It was in this environment that the EU first began to respond to cyber threats.

These threats were described in socio-economic terms: copyright breaches, payment card fraud, illegal drug production, libel and even the protection of minors. Due to a combination of competences restricted by successive Treaties and the division of policy responsibility initiated by the Maastricht Pillar system, the EU addressed cyber security concerns through an economic lens, establishing an *interpretation* of the problems. This influenced the manner in which these issues were approached and conceptualised. Instead of tackling issues such as distributing harmful content online, credit card fraud or libel as solely criminal justice problems requiring criminal justice solutions, the EU approached them by seeking to minimise their impact on the economic potential of cyberspace. As stated explicitly by the Commission in *COM (1996) 487 on Illegal and Harmful Content on the Internet* "the presence of illegal and harmful content on the Internet has direct repercussions on the workings of the Internal Market" (European Commission, 1996a, p. 4). These threats were to be managed in such a way as to cause minimal damage to the continued operation of the Internal Market. This management and limitation of impact created a policy path which would influence the nature of the EUCSS in 2013. That policy does not establish methods or techniques for seeking out malicious actors and criminal activity. Rather it seeks to ensure the continued functionality of cyberspace and the Internet (European Commission, 2013a, p. 5). The important point to make at this juncture is that Union competences locked a socio-economic discourse in place despite themselves being formalised *after* the initiation of EU interest in ICT and cyber issues. This demonstrates that institutional arrangements such as the EU's system of competences can have significant effects on pre-existing policy paths.

The chapter provided tabular analyses comparing important *acquis* milestones with the EUCSS. This provided evidence of the linear connection between the EUCSS and its predecessors without lapsing into determinism or historical causality. There is a linear progression between the earliest cyber security *acquis* and the EUCSS of 2013, showing that these documents are part of an underlying discourse.

The chapter also showed that the socio-economic interpretation was cemented in 2001 with the publication of the NIS Proposal. This was the first publication which includes recognisable cyber security elements. Despite containing specific threat typologies and a codified definition of cyber security, the Proposal established the EU's approach as one which sought to ensure the continued exploitation of this developing commercial domain. NIS was seen as a tool for ensuring economic growth and social advantage, as opposed to a function of national security or defence.

The identification of the initiation of path dependencies in the timescape is important for a number of reasons. First, these paths were instrumental in setting the tone for the incremental development of a socio-economic cyber security discourse. Second, while a purpose of this thesis is to identify those institutions which have had an influence on the EU's cyber security discourse and policy-making, it is just as important to identify *why* such a discourse developed. The convergence of the establishment of the Single Market in 1985 and the signing of the Single European Act, with its explicit security restrictions, represents the point at which that socio-economic cyber security position began. This is an important point in an HI analysis: the establishment of path dependencies. Once these paths are in place – i.e. once particular policy choices have been made – there then follows a period of consolidation and policy entrenchment. This consolidation will be the focus of the following chapter.

At this point in the analysis it would be too early to declare that the path to the EUCSS of 2013 was laid out in any deterministic manner. The seeds were nevertheless planted in the mid-1980s. The clarification in Treaties of the EU's security competences as well as the initiation of the Single Market established path dependencies which, as will be shown in the following chapters, would prove highly resilient (Pierson, 2000, p. 263). From an HI perspective the principles and procedural norms established between 1985 and 2001 created strong path dependencies, which would be consolidated in later years. This process of consolidation occurred between 2002 and 2006.

Chapter 7 | Policy Consolidation 2002-2006

7.1. Introduction

Chapter 6 showed how cyber security policy paths were established between 1985 and 2001. Following this establishment EU cyber security policy entered a period of consolidation or institutional stasis between 2002 and 2006. The discourse begun in 1985 became embedded in subsequent policy choices. Evidence of this inertia and bedding-in can be found in the initiation of specialised agencies whose mandates focused on two core facets of EU policy: providing channels for information-sharing and the facilitation of co-operation between the EU's Member States and the private sector.

The predominance of economic and criminal justice matters in cyber security policy was established in the NIS proposal of 2001. To operationalise this policy two agencies were established. A "high-tech crime" centre (HTCC) was founded at Europol with the dedicated aim of tackling online criminal activity and the online exploitation of children. Its goal was to act as a hub for criminal intelligence gathered from across the Union. In a similar vein, in 2004 the European Network and Information Security Agency (ENISA) was established at the Greek city of Heraklion on the island of Crete. ENISA's goal was and is to act as an advice broker, ensuring information and best practice is disseminated to all who would benefit from it. ENISA and the HTCC were used to operationalise what was becoming the most important aspect of Union policy in this field – facilitating co-operation.

Despite this ideational inertia, the period 2002-2006 represents a paradox in EU cyber security policy development. While the underlying policy discourse continued unchanged, the period saw a shift in dynamic on the part of the EU's approach to cyber security as a whole. The NIS Proposal of 2001 contained a highly prescriptive approach to cyber security. Specific solutions were proposed, including installing secure servers and up-to-date anti-virus software. This reflected a very proactive approach to the field. By 2006 this had been tempered, and shifted to a more arms-length pattern of solution-building. Reference to specific technological measures disappeared from the *acquis* in favour of softer approaches such as recommendations for co-operation and tools for information-sharing.

The evidence for this shift in dynamic is to be found in two places: the content of *acquis* produced between 2002 and 2006; and the methods employed by the two operational agencies initiated in this phase. An examination of the relevant *acquis* demonstrates that the language used changed to a softer tone. Instead of being instructed to, for example, install anti-virus software or secure DNS servers, entities were *invited* and *encouraged* to co-operate and take part in solution-building.

This new approach is epitomised in the remit and actions of the HTCC and ENISA. The HTCC did not carry out arrests for computer-related crime. It analysed criminal intelligence on behalf of Member states. Similarly, ENISA did not provide security *per se*. It is not an agency which stipulates solutions or implements particular tools for cyber security. ENISA's purpose was and continues to be to act as a hub for information and best practice exchange. The new dynamic and facilitative role was formalised in 2006, with the publication of the first recognisable strategy addressing cyber security issues, the *Strategy for a Secure Information Society*. This shift in dynamic is noteworthy because it occurred against the backdrop of a static policy discourse. As will be shown in this chapter, the five core ideational elements of the EU's cyber security discourse continued to influence policy development in this period.

The chapter is divided into four sections. The second section will examine the initiation of the HTCC and ENISA. It will explore the role of these two agencies in continuing core ideational elements of EU cyber security policy. The section will also examine the aims, mandates and activities of these agencies to illustrate how the EU shifted from a prescriptive to a softer approach in this period.

The third section of the chapter will examine the impact of the publication in 2006 of the *Strategy for a Secure Information Society* (SSIS). A content analysis of the SSIS will demonstrate both the continuity of the underlying policy discourse from the previous phase as well as the EU's new dynamic in cyber security. Despite continuing a focus on the five core ideational elements which underpin the EU's discourse in this sector, the SSIS removed much of the highly prescriptive, definition-introducing content of the 2001 Proposal. The SSIS instead provided a softer, facilitative approach. A fourth section concludes the chapter.

Throughout the chapter the continuity of the five ideational elements will be evidenced in order to demonstrate their continuing influence on policy-making in this area. In addition

to being major milestones for the development of cyber security policy, the nature of ENISA and the content of the SSIS reflect the five core ideational elements inherent to cyber security policy. Co-operation is of particular significance, given ENISA's *raison d'etre* as a broker for information-sharing and the subtitle of the SSIS being "Dialogue, Partnership and Empowerment".

7.2. Operationalising Cyber Security Policy

7.2.1. Europol and the Fight against Cybercrime

Europol became fully operational in 1999 (Europol, 2013b) as a centre for co-ordinating co-operation between Member States' police forces. Its purpose was to combat terrorism, drug trafficking and international crime (Europol, 2013c). Prior to the establishment of Europol, international measures to tackle such criminal activity were carried out on bilateral bases. The disadvantage with this approach was that, in the case of serious and organised crime, criminal groups "are multinational and are comprised of multiple nationalities" (Interview, Senior Official, Europol, 2014). Establishing a bilateral police mission, with the involvement of only two Member States, created a very limited perspective on criminal networks and their activities. Europol was able to address this issue by removing the need for a multitude of separate arrangements (Interview, Senior Official, Europol, 2014). Member States could pass criminal intelligence information to Europol's specialist research units where that intelligence would be analysed alongside contributions from other Member States.

As this agency matured, and in recognition of the changing nature of criminal activity, in 2002 a "high-tech crime centre" (HTCC) was established (Europol, 2013d). The remit of the HTCC was focussed on three specific areas of criminal activity described as "crime areas in which the Internet plays a key role" (Europol, 2013d). These areas were computer-related crime, payment card fraud and the protection of children from online exploitation.

The establishment of a specific unit dedicated to criminal activity where the Internet plays a role demonstrates not only the importance placed on cyber-crime by the EU at the time, but also the socio-economic focus of EU cyber security policy as a whole. Economic interaction, particularly card payments, was being protected so that the trust and uptake of digital media could be improved. Similarly, protecting children online demonstrated the EU's resolve to address the social aspect of the increased use of digital and online

technology. Payment card fraud emphasised the EU's commitment to treating NIS issues as criminal acts affecting the Union's economic development. The expansion of Europol's remit into the investigation of online child sexual exploitation demonstrates a widening of the issues that the EU considers a part of cyber security. Acts that cause harm not just to physical objects but to people were being included in a wider approach (European Commission, 2005, p. 3). The aim was to build trust in the system, by "making the Internet safer from fraudsters, harmful content and technology failures to increase trust amongst investors and consumers" (European Commission, 2005, p. 5).

The methods employed by Europol in this new high-tech crime centre were the same as those for its other units. The HTCC, and Europol as a whole, was not an agency dedicated to policing Europe. This task was left to the Member States. Europol *assisted* Member States in their responsibilities by facilitating information-sharing. It provided assistance and expertise in the form of data and evidence collection and analysis. The results of these analyses are returned to the Member States, who retain executive judicial authority. In short, it was Member State police forces, not Europol, who carry out arrests and "kick down doors" (Interview, Senior Official, Europol, 2014). This pattern of providing analysis and expertise continued into the HTCC.

This is a core element of the EU's facilitation of co-operation. It demonstrates the nature of the role that the Union was establishing for itself in cyber security between 2002 and 2006. The EU – via Europol – sought to enable national police forces to co-ordinate their information and efforts more efficiently by providing a central nexus for criminal intelligence and analytical expertise. This is not an executive role for the EU, but a facilitative one, a softer approach to security as opposed to a harder hands-on approach inferred in the 2001 NIS Proposal.

During the 2002-2006 phase, therefore, the EU was seeking avenues to promote joint-working and information-sharing – i.e. co-operation – amongst its Member States as well as those entities with a vested interest in a safe and secure European digital space. Co-operation between entities was deemed vital not just to ensure security of systems and networks, but also to ensure trust in those systems (European Parliament & Council of The European Union, 2004, p. 3). The HTCC was an important part of this mechanism.

To help further these goals, in 2004 the EU established an agency to handle network and information security itself, as opposed to concentrating on cyber-crime. This body was named the European Network and Information Security Agency (ENISA).

7.2.2. The European Network and Information Security Agency

ENISA was established in 2004 with the objective of enhancing the capabilities of the EU, its Member States and the business community to research, respond to and prevent NIS problems (ENISA, 2005). Its mission is to achieve a high level of network and information security (NIS) within the EU by building on national and Community efforts in the field (European Parliament & Council of The European Union, 2004, p. 2)[40]. It was also intended to operate as a point of reference for advice and information. This function was provided not just to EU institutions and Member States, but also to other relevant stakeholders including those in the private sector. This was due to the recognition that the electronic networks and services were, by 2004, largely privately owned (European Parliament & Council of The European Union, 2004, p. 2).

ENISA's mandate and work was very specific. The agency was (and still is) primarily concerned with protecting the EU's open market. As described by Purser (Interview, Purser, ENISA, 2014) "[ENISA] is concerned with businesses [and] the public sector but not with the military and not with cyber-crime directly". This demonstrates a clear distinction between addressing the economic impact of cyber security, and tackling criminal justice or defence issues. ENISA's mandate specifically excludes defence (Interview, Helmbrecht, ENISA, 2014). This is further evidence of the priority placed on economic matters by the Union as a whole: a specialist agency was set up to support cyber security solutions intended to mitigate threats to the economic and functional viability of the Single Market.

That being the case, ENISA, as an agency, does not provide security *per se* (Interview, Purser, ENISA, 2014; Interview, Rönnlund, DG Connect, 2015). Instead it describes itself as an "Advice Broker" (ENISA, 2005). It is a "mechanism for enabling stakeholder groups throughout Europe to work with each other" (Interview, Purser, ENISA, 2014). As such it operates as an intermediary or conduit for information to and from its various stakeholder groups and the European Commission. It ensures that experiences and best practice are

[40] This Directive was repealed in 2013 and replaced with (European Parliament and Council of The European Union, 2013a) Although the founding Regulation was repealed, its replacement did not substantially alter the principles under which ENISA was to function.

effectively shared and communicated. To facilitate this, ENISA has gathered together a library of national and international cyber security strategies and published them online (ENISA, 2013; Interview, Senior Official, DG HOME, European Commission, 2014). An implementation guide was published alongside this, proposing specific actions intended to aid the development of a comprehensive cyber security strategy (Falessi et al., 2012). ENISA also helps its stakeholders address, respond to and prevent NIS problems through publishing advice and assistance (Robinson, 2012, p. 165). It also produces guidelines covering a range of issues including best practice regarding minimum security standards (ENISA, 2011a).

In terms of facilitating co-operation, there are three types of activities undertaken by ENISA. One is joint-working between the agency itself and other non-EU bodies. This includes the NATO Co-operative Cyber Defence Centre of Excellence (CCDCOE), based in Tallinn. Utilising the expertise of both agencies, a major project looking at tackling botnets was undertaken where the CCDCOE provided legal expertise surrounding tackling such illegal networks, and ENISA provided the technical support (Interview, Traat and Ristikivi, 2014).

A greater emphasis, however, is placed on the role of ENISA as a co-ordinating agency. An important example of such a role is the staging and management of biannual cyber security exercises (Interview, Purser, ENISA, 2014; ENISA, 2005). These exercises simulate cyber incidents targeting critical information infrastructures underpinning EU functionality such as the banking sector or communications networks. The object is to examine participants' responses, collective and individual practices and co-operative capabilities. Named "Cyber Europe", the first exercise took place in November 2010, and brought together representatives from 22 Member States and eight observer nations (ENISA, 2011b, p. 3). Two years later Cyber Europe 2012 built on the findings of its predecessor and brought private stakeholders into the simulations. These included financial institutions and internet service providers (ISPs) (ENISA, 2012, p. 5). ENISA also facilitated a transatlantic version of the exercises in 2011 known as Cyber Atlantic. This exercise was carried out in co-operation with the EU-US Working Group on Cybersecurity and Cyber Crime (ENISA, 2011c).

The main findings of all of these exercises were that, while some work was needed to build capabilities, more training and information-sharing *between* actors was needed to raise

both awareness of existing measures across all stakeholders, and also the level of collective security in the face of large-scale incidents. These exercises demonstrate ENISA's, and by extension the EU's, commitment to facilitating co-operation and co-ordinating pan-European responses to cyber security incidents.

A third aspect of ENISA's co-ordinating and co-operative function, and a core aspect of ENISA's work overall is harmonisation (Interview, Purser, ENISA, 2014). Harmonisation has been an important policy aim since 2002, when it was recognised in a Directive of that year that a regulated approach focusing on access to, and interconnection of, electronic communications networks and associated facilities will help to develop

> relationships between suppliers of networks and services that will result in sustainable competition, interoperability of electronic communications services and consumer benefits (European Parliament and Council of the European Union, 2002b, p. 11).

The issue was that national and private sector initiatives to mitigate cyber security risks were often undertaken individually. Consequently they had differing priorities and solution bases. In order to effectively establish a pan-European, or at least an EU-based, response to cyber security issues, the various initiatives in place needed to be compatible with one another and meet certain collective minimum standards. An example of such work was that undertaken within the Computer Emergency Response Team (CERT) community. ENISA facilitated the development of CERT documentation, which was then disseminated to all the Member States, providing a common platform (Interview, Purser, ENISA, 2014).

ENISA serves as an operational exemplar of the continued importance placed by the EU on co-operation, and a manifestation of the Union's role as a facilitative actor. As a method of approaching cyber security challenges arising from an increasing use of digital media in all walks of life, co-operation between interested entities was crucial for the EU at this time. Furthermore, because cyber security was becoming an increasingly international concern, addressing these issues at the EU level adhered to the principle of subsidiarity. That principle, contained in Article 3b of the Treaty of Maastricht, stipulated that the Union will involve itself in an issue

> only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects

> of the proposed action, be better achieved by the Community (European Union, 1992, p. 13).

In short, the Union will become involved if it can be more efficient or effective in achieving specific objectives (Follesdal, 2013, p. 1). Because it was recognised in this 2002-2006 phase that cyber security challenges were inherently international in nature, it made more sense for the EU to facilitate resolving those challenges than for individual Member States to engage in them separately.

Although the establishment of the HTCC at Europol and ENISA were major milestones in the EU's cyber security policy-making process, both of these events reflected a shift in the EU's handling of that policy. The NIS Proposal of 2001 was highly prescriptive in nature, going so far as to specify particular solutions to particular problems. By 2004, however, this approach had shifted dramatically to a more arms'-length approach to cyber security. The EU would facilitate the sharing of information and help to put interested parties in contact with one another. Neither the HTCC nor ENISA took any form of direct action to solve cyber security issues. The HTCC functioned under the operational parameters of its parent agency, Europol. Criminal intelligence was fed to its processing units from across the EU's membership and beyond, where it was analysed and fed back. It was, however, for the Member States to decide how to use that information and ultimately it was the Member States who carried out arrests (Interview, Senior Official, Europol, 2014). Similarly, ENISA did not and does not secure anything (Interview, Purser, ENISA, 2014). It ensures that all relevant entities within its purview – the formal institutions of the EU and the Member States – have access to the information and resources they need to be able to function in a safe digital environment. This is a very different, softer dynamic to the prescriptive policy of the NIS Proposal. This new dynamic was codified in the publication of the first approved cyber security strategy of the EU[41]: *COM (2006) 251 – A Strategy for a Secure Information Society*.

7.3. A Shift in Approach but not Discourse: The 2006 Strategy for a Secure Information Society

This period of consolidating EU cyber security policy closed with the publication in 2006 of the *Strategy for a Secure Information Society – Dialogue, partnership and*

[41] The NIS Proposal of 2001 was just that, a proposal. Although cited by the EU as a document in cyber security *acquis*, it, and its contents, were never formally accepted as policy.

empowerment (here referred to as the SSIS). The SSIS is an important document in the incremental, linear development of EU cyber security policy for three reasons. First, it was the first formally approved strategy document produced by the EU in this policy area. Previous *acquis* were either position papers on illegal and harmful content (European Commission, 1996a) or proposals for strategy documents that were never formally approved (European Commission, 2001a). To have a formal policy approved and accepted by the EU's constituent actors was a significant step in cyber security policy development. Second, the SSIS demonstrated continuity of policy aims, in particular the five core ideational elements of the EU's discourse. These are a focus on economic maximisation, engendering trust, protection of fundamental rights, tackling cyber-crime and achieving these through co-operation. Third, the SSIS codified a shift in the EU's approach to cyber security. This shift was away from prescriptive instructions, such as those in the 2001 NIS proposal, to an arms'-length handling of cyber security issues.

7.3.1. Ideational Continuity in the Strategy for a Secure Information Society

The 2006 SSIS continued a number of important themes established in 1996 and 2001. This further supports the position that cyber security policy-making was an incremental and linear, but not deterministic process. Economic security and the viability of the Single Market, as well as the protection of privacy, fundamental rights and information integrity, are goals which endure throughout the policy-making timescape. The SSIS should therefore be considered the third step in the incremental policy-making process.

The SSIS was intended to revivify efforts in NIS, (European Commission, 2006a, p. 3) and act as a successor to the 2001 Proposal. It directly quoted its predecessor in a number of key areas, including the definition of network and information security (European Commission, 2006a, p. 3). It continued to prioritise economic viability, stating that "the relevance of the ICT sector for the European economy and for European society as a whole is incontestable" (European Commission, 2006a, p. 5) The SSIS supports this claim by stating that, by 2006, ICT was responsible for nearly 40% of economic productivity (European Commission, 2006a, p. 5). In addition, security breaches eroded trust in electronic communications and citizens' willingness to invest in and use online technologies. This would be detrimental to the EU's economic development. Furthermore, the EU's commitment to fighting cyber-crime continued as NIS threats had the potential to affect citizens in their everyday lives (Council of The European Union,

2008, p. 1). This commitment would be achieved through the co-operation of interested parties.

This continuity also extended to the other core ideational elements underpinning the EU's cyber security discourse. What began as the protection of human dignity in 1996 (European Commission, 1996a, p. 3) would eventually be codified in the European Convention on Human Rights, a core feature of the 2001 NIS Proposal (European Commission, 2001a). By 2006, it was recognised in the SSIS that, in addition to protecting such fundamental rights, ensuring the security of digital infrastructures was instrumental to achieving this (European Commission, 2006a, p. 5). This goal was carried forward into the EUCSS of 2013 (European Commission, 2013a, p. 3,15).

There is a similar linear process for ensuring economic security, particularly to counter financial fraud. As early as 1996 the pirating of credit cards was a recognised downside of increasing ICT connectivity (European Commission, 1996a, p. 3). As technology and the internet developed, by 2006 malicious software (malware) had been produced that could seek out digital records and access personal financial data (European Commission, 2001a, p. 10, 2006a, p. 4). By 2013 a tenth of all Internet users had been the victim of some kind of online fraud (European Commission, 2013a, p. 3).

This continuity of both policy concepts and content can be seen in Table 7-1 below. The table serves to highlight the conceptual and content continuity between these core documents of the EU's discourse and the final EUCSS of 2013.

Table 7-1: Continuity in Cyber Policies 1996-2013

COM (1996) 487 (European Commission, 1996a)	***COM (2001) 298*** (European Commission, 2001a)	***COM (2006) 251*** (European Commission, 2006a)	***EU Cyber Security Strategy*** (European Commission, 2013a)
national security (instructions on bomb-making, illegal drug production, terrorist activities); *protection of minors* (abusive forms of marketing, violence, pornography);	…there are growing concerns about national security as information systems and communication networks have become a critical factor for other infrastructures (e.g. water and electricity supply) and other markets (e.g. the global finance market).	*Cyber defence is not addressed in this document. This is due to a scaling back of direct proactive engagement on the part of the EU and a stricter adherence to the letter of the competences. See Section 7.3.2 of this chapter for a broader discussion of this phenomenon.*	Cybersecurity efforts in the EU also involve the cyber defence dimension. To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyber defence capability development should concentrate on detection, response and recovery from sophisticated cyber threats
protection of human dignity (incitement to racial hatred or racial discrimination);	*Although protection of human dignity is not specifically mentioned in COM (2001) 298, adherence to the European Convention on Human Rights and the EU's Charter of Fundamental Rights is mentioned. Human dignity is a core element of both these documents*	A breach in NIS can generate an impact that transcends the economic dimension. Indeed, there is a general concern that security problems may lead to user discouragement and lower take-up of ICT, whereas availability, reliability and security are a prerequisite for guaranteeing fundamental rights on-line.	Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred). The EU international engagement in cyber issues will be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights.
economic security (fraud, instructions on pirating credit cards);	Unlawful interception can cause damage both through invasion of the privacy of individuals and through the exploitation of data intercepted, such as passwords or credit card details, for commercial gain or sabotage. This is perceived to be one of the biggest inhibitors to the take-up of e-commerce in Europe.	[Malware] is becoming a vehicle for viruses and fraudulent and criminal activities, such as spyware [and] phishing - a form of Internet fraud aiming to steal valuable information such as credit cards, bank account numbers, user IDs and passwords.	Across the EU, more than one in ten Internet users has already become victim of online fraud.
information security (malicious hacking);	Some unauthorised intrusion is motivated by intellectual challenge rather than monetary gain. However, what began as a nuisance activity (often described as 'hacking') has highlighted	Data are illegally mined, increasingly without the user's knowledge, while the number of variants (and the rate of evolution) of malware is increasing rapidly.	Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored

	the vulnerabilities of information networks and motivated those with criminal or malicious intent to exploit these weaknesses.		activities in cyberspace poses a new category of threats for EU governments and companies.
protection of privacy (unauthorised communication of personal data, electronic harassment);	Protection of privacy is a key policy objective in the European Union. It was recognised as a basic right under Article 8 of the European Convention on human rights, Articles 7 and 8 of the Charter of Fundamental Rights of the European Union 21 also provide the right to respect for family and private life, home and communications and personal data.	Promote diversity, openness, interoperability, usability and competition as key drivers for security as well as stimulate the deployment of security-enhancing products, processes and services to prevent and fight ID theft and other privacy-intrusive attacks.	Protecting fundamental rights, freedom of expression, personal data and privacy: Cyber security can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems.
intellectual property (unauthorised distribution of copyrighted works, e.g. software or music)	Unauthorised access into computer and computer networks is usually done with malicious intend to copy, modify or destroy data.		Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), [and] content-related offences.

The table demonstrates a conceptual link between the core elements of the original Commission Communication of 1996 on illegal and harmful content, its successor in the 2001 NIS Proposal, the SSIS of 2006 and the EUCSS of 2013. This demonstrates the linear connection between these documents and their function as non-deterministic stepping stones from the inception of policy in this sector in 1985 to the finished EUCSS of 2013.

7.3.2. A New Dynamic for Cyber Security

While there was clear continuity of policy discourse between 1985 and the 2002 SSIS there was one significant change. Gone were the detailed, specific typologies of threats and the apportionment of specific responsibilities for addressing those threats. By removing these specifications for action the EU was codifying its new, looser, arms'-length approach to cyber security which had been developing since 2002. This new dynamic was exemplified by the Union setting itself up as a facilitative actor rather than an entity which actively secures things. In short, what differentiated the 2006 *Strategy for a Secure Information Society* from its 1996 and 2001 predecessors was the manner in which the EU sought to achieve its goals. Instead of specifying solutions and expecting interested parties to implement them, the EU advocated a softer, less prescriptive method.

The SSIS included a three-pronged approach to NIS issues (European Commission, 2006a, p. 3). The second and third prongs have their origins in the proposal of 2001; a regulatory framework sought to ensure a competitive market within the EU and combatting cyber-crime was prioritised. At first glance this approach may seem similar to previous policies. However, on closer examination it is the first prong, the "specific NIS measures", which provides the greatest contrast between EU policy in 2001 and 2006. The 2006 approach was characterised by a shift towards greater inclusiveness on the part of all entities with a vested interest in cyber security. This can be seen in the language used to describe these measures. In 2006 stakeholders such as Member States, the private sector and the research community would be "invited" to enter into strategic partnerships (European Commission, 2006a, p. 8). The private sector was also "invited to disseminate good security practice within its community to establish baseline levels for security and business continuity (resilience)" (European Commission, 2006a, p. 9). These invitations are a stark contrast with the more definitive language of the 2001 NIS Proposal. There it was stated that operators should secure networks "as they are required to do under *Directive 97/66 EC [on Data Protection in Telecommunications]"* (European Commission, 2001a, p. 10) and that a

balance between network protection and the advantages of open access "must be achieved" (European Commission, 2001a, p. 12). By 2006 there had been a softening of tone and language to develop an environment of encouragement and partnership.

To achieve these goals the Commission called upon ENISA, in its role as an advice broker, to provide the focal point in various efforts. These included promoting co-ordination and serving as a centre for co-operation, as well as facilitating information-sharing and the exchange of best practice (European Commission, 2006a, p. 6). One method employed by ENISA to encourage such co-operation was the organisation of the Cyber Europe and Cyber Atlantic international exercises (European Commission, 2009a, p. 9) examined in the Section 7.2.2 of this chapter.

What the actions of ENISA and the EU's policy framework at this time demonstrate is that the wider goal in this period of cyber security policy development had altered. The goal by 2006 was not to establish, identify and publicise specific EU definitions of terms and challenges, nor was it to prescribe specific courses of action. Instead, the aim was to foster an international culture of network and information security (Robinson, 2012, p. 165; European Commission, 2006a, p. 4). In this culture all stakeholders would be involved, and NIS seen as a virtue and commercial opportunity. It is not by accident that the 2006 Strategy was subtitled "Dialogue, Partnership and Empowerment". The tone of the SSIS is one of ensuring not only that all actors fulfil their responsibilities, but also that those actors are given support and resources – that they are empowered (European Commission, 2006a, p. 6,10). Through such measures as establishing ENISA and the HTCC at Europol, the EU had positioned itself as a facilitator of that dialogue, partnership, and empowerment, rather than a prescriptive taskmaster. Core ideas were consolidated, but the approach had shifted.

What makes the SSIS stand out as a milestone in the linear policy-making process, therefore, is not simply that it was the first formally accepted policy document in this field. It stands out because it was different from its predecessors yet maintained the continuity of a policy discourse based on five core ideas. As a policy document it established a new paradigm of EU involvement in cyber security, one where direct action is minimised and the EU's function as a facilitative actor is emphasised. These differences are more than simple updates of policy to take into account new and emerging challenges or developments in the field since 2001. They are differences in approach resulting in a shift away from a heavy-handed, proactive approach towards a more reserved one recognising the roles of the various stakeholders involved (European Commission, 2006a, p. 6). What

is significant is that this shift in dynamic occurred without any change in the policy's ideational foundations. Cyber security policy was still focussed on ensuring economic viability, promoting trust, protecting fundamental rights, tackling cyber-crime and promoting co-operation.

The EU's co-operative zeal was not restricted to facilitating joint-working between Member States and external actors, however. In 2002, there was a recognition that better co-operation was needed between the three Pillars of the EU's policy-making architecture. There was a particular focus on promoting joint-working between the Pillars of Justice and Home Affairs – which focused on criminal justice matters – and the Communities Pillar which managed the Single Market (Council of The European Union, 2002c, p. 2). In a meeting of the Council of the European Union's Committee on Telecommunications in January 2002, it was acknowledged that better communication and co-ordination between the two Pillars was required to reduce the likelihood of duplication of efforts in cyber security. This was a particular issue given the prevalence of threats which were both criminal acts *and* which affected the resilience of the Single Market (Council of The European Union, 2002c, p. 3). The attempt to mitigate such a risk of duplication was one of the defining characteristics of the years between 2007 and 2013, the final phase of policy development. Even in 2002 it was recognised that more needed to be done to ensure adequate pooling of resources where issues arose that crossed Pillar boundaries, such as cyber security. This particular set of Council Conclusions is also noteworthy for including the first mention of the term "cyber security" in Union *acquis* (Council of The European Union, 2002c, p. 2). From this point the term begins to be used more frequently to refer to the totality of security risks to and from cyberspace, although it does not enter common policy jargon for some years.

7.4. Conclusion

Chapter 6 showed that the years up to 2001 were defined by the initiation of important path dependencies in the EU's cyber security policy-making process. Chapter 7 has shown that years between 2002 and 2006 were characterised by institutional stasis and a bedding-in of those policy paths. These paths were a focus on economic maximisation, the protection of rights, tackling cyber-crime to build trust in the digital sphere and achieving these through facilitating co-operation. The chapter also showed that this final element developed beyond a simple policy goal to become a defining feature of the EU's role in tackling cyber security issues.

The period between 2002 and 2006 was marked not only by policy consolidation but also by important developments. From an institutionalist perspective, the years following the publication of the Commission's NIS Proposal, with its direct prescriptions for specific action such as firewalls and anti-virus software, would logically be a period of entrenchment of these policy ideas. Paradoxically however, the 2002-2006 phase was characterised by a stepping back of direct Union action in this field and the adoption of a more distant, arms'-length approach to the same security challenges. The *acquis* published between 2002 and 2006 pointed less to a desire to proactively engage in solution-building, than to position the Union as a facilitative actor. Its role in this period became that of an advice broker, ensuring information and best practice regarding national and private sector solutions were shared, rather than setting out, prescribing and promoting those solutions. Although cyber security would remain an important aspect of the functioning of the internal market, the manner in which the EU achieves this, and the role it plays in doing so, has evolved from its beginnings in 1985. That role was to promote co-operation between interested parties and during this period the EU positioned itself as a facilitator of that co-operation.

The chapter also demonstrated that to do this two dedicated agencies were established: the High-Tech Crime Centre at Europol and the European Network and Information Security Agency. The role for both of these agencies was to support Member States and international liaisons by providing fora for sharing information relating to cyber security issues. Through publishing advice on best practice and carrying out major international simulations of cyber incidents, ENISA has established itself as an important hub in European cyber security generally.

This trend of brokering advice and co-ordinating co-operation was exemplified in the *Strategy for a Secure Information Society,* published in 2006. This Strategy was an important step in the incremental process of cyber security policy-making for two reasons. Not only did it continue policy paths established between 1985 and 2001, bedding these into the policy discourse, but it also codified a new arms'-length approach to cyber security. Gone were detailed definitions of cyber security threats and solutions to those threats. The SSIS advocated empowering and supporting entities to fulfil their own responsibilities and codified the role of the EU in facilitating that co-operation.

The SSIS therefore represented a change in the manner of the EU's approach to cyber security and formalised its facilitative role. It also represented ideational continuity. This

continuity demonstrated the inertia of paths laid down in the earliest period of policy development, 1985-2001, highlighting the linearity of the EU's cyber security policy. That linearity and inertia would be subject to severe stresses in subsequent years. The influence of those stresses is the subject of the following chapters.

Chapter 8 | Punctuated Equilibrium Part 1: The Influence of Exogenous Institutional Stresses on EU Cyber Security Policy

8.1. Introduction

The period between 2007 and the publication of the EUCSS in 2013 is the most vibrant and important in the EU's cyber security policy-making timescape. Of particular significance is the occurrence between 2007 and 2009 of a series of major events and crises, acting as punctuation points in the policy-making process. These events warrant separate analyses due to their complexity and the scale of their influence on this particular policy area. The events galvanised Union interest in cyber security in a manner not seen before. As a consequence, between 2007 and 2013, over 50% of Union *acquis* relating to cyber security (73 of the total of 143 documents) were released during this period alone. Most importantly, they ultimately led to the development of the European Union's *Cyber Security Strategy* (EUCSS) which was published in 2013 (European Commission, 2013a). Evidence gathered from interviews and analyses of Union *acquis* will be presented here to demonstrate that these major catalytic events had a profound influence on EU cyber security policy.

This chapter will examine the influence of two of these events, the triggers for which were exogenous to the EU: the cyber-attack on Estonia in 2007; and the financial crisis of 2008. The direct consequence of these events was an increase in political interest in critical information infrastructure protection (CIIP) and resilience in order to maintain the viability of the EU's digital marketplace. Despite originating outside the Union's geopolitical boundaries these events necessitated responses from the EU.

The chapter is divided into four sections. The second section examines the distributed denial of service (DDoS) attacks experienced by Estonia in the summer of 2007. A particular problem for the EU with regard to these attacks was its lack of competence in security matters. The chapter argues that this complication required the EU to *interpret* important international events such as the Estonian attack as socio-economic issues. By interpreting that event as a threat to the internal market, the EU was able to engage with the issue and undertake measures to bolster the security of digital infrastructures. This is the same interpretive process undertaken in previous years. The DDoS attack experienced by Estonia was described as an existential but *economic* threat (Interview, Smith and Jones, eu-LISA, 2014; European Commission, 2009a, p. P.2). Economic threats are issues where

the EU can act. Direct threats to national security, by contrast, are sectors where Union action is severely restricted.

The third section of the chapter will examine the effect on cyber security policy of the commencement of the global financial crisis in 2008. This event did not need the same creative interpretation as the Estonian DDoS attacks. Because the EU is an economic entity, any major events which affected commercial growth and productivity, regardless of where they originated, came under its remit and competence. The point will be made in this chapter that the financial crisis of 2008 generated a repeat of processes and policy choices initiated in the 1980s. In both periods Europe was facing financial difficulty and turned to digital industries as sectors where growth and employment could be stimulated. In both cases political interest in cyber security increased, leading to a greater dynamism and willingness to develop policy.

The chapter will argue, however, that what did *not* occur was a change in the EU's underlying cyber security discourse. Instead, that discourse became further entrenched as a result of the EU's need to interpret the Estonian attacks as economic threats. The result of this entrenchment was that the EU's socio-economic cyber security discourse, as well as the five ideational elements which underpinned it, continued on previously established paths. This occurred despite a cyber-attack on a state taking place and the commencement of a financial downturn which affected markets around the world. This entrenchment infers an institutional "stickiness" (Pierson and Skocpol, 2002, p. 7) inherent to those paths, which meant that they were strong enough to withstand major events and crises which would otherwise cause policy change.

8.2. Crisis 1 – The 2007 Cyber Attacks on Estonia

At the beginning of April 2007, local authorities in Tallinn, Estonia's capital, chose to move a Soviet memorial to the Second World War from the centre of the city to a new location on its outskirts (Gaycken, 2011, p. 170). This act was considered by the Russian minority in the country to be an insult. Public protests erupted in the city which on 26th and 27th 2007 April turned violent. There were around 1300 arrests, 100 injuries and one fatality (Rid, 2013, p. 6).

Alongside these public protests, on 26th April a series of cyber incidents began to take place, targeting the Estonian Parliament and other institutions such as banks, ministries and media outlets. The incidents escalated over a period of four weeks. On 4th May local domain name system (DNS) servers were targeted by low level denial of service attacks

(Schmidt, 2013, p. 181; Rid, 2013, p. 6). Between 9th and 11th May these had escalated to distributed denial of service (DDoS)[42] attacks targeting government websites and Estonian financial services and banks. By 15th May, in a third wave, perpetrators began to use a system of botnets to increase the impact of these DDoS attacks (Schmidt, 2013, p. 181).

According to Rid (2013, p. 6) the material impact of the DDoS attack was relatively minor. Websites were either defaced or rendered inoperable and elements of the Estonian banking sector were unavailable for a total of four hours over two days. The political fallout of the incident however, was substantial. Critical elements of the highly-developed digital infrastructure of a small country were temporarily shut down with a sophistication which implied foreign state involvement (Bucci, 2012, p. 59). The Estonian government considered this incident an armed attack on its sovereignty, and sought to invoke Article V of the NATO Treaty. This article stipulates that an attack on one Alliance member is an attack on all. There was, however, no consensus amongst NATO allies that the hacks constituted armed attacks and so Article V was not brought into play.

Had Article V been triggered, the potential consequences would have been severe due to suspicions around the source of the hacks. Because of the timing of the attacks and the complexity involved in their perpetration, the conclusion was drawn that Russia, or Russian-backed hackers, were responsible. Analyses of the hacks have not been able to categorically detect direct Russian government involvement (Fidler, 2012, p. 77), but the coincidence was considered too great to ignore. This incident thrust cyber security, particularly government- or state-sponsored activities, into the public domain and up the ladder of political discussions. If nothing else, the incident eroded trust (Rid, 2013, p. 31) in both the digital networks' capacity to withstand such intrusions and national governments' capacities to avert them.

This incident was an important milestone in cyber security history itself. Due to circumstantial evidence pointing to Russia being the originator of the attacks, "Estonia 2007" was the first publically acknowledged instance of state-on-state computer network operation (CNO) and elevated cyber security, and the concept of "cyber warfare" to the highest national policy discussions. For the EU, the attacks highlighted systemic weaknesses in national and European digital infrastructures which could potentially have a cascading effect through its economic area.

[42] A distributed denial of service attack (DDoS) involves a website or host server being flooded with automated, artificial requests for access. The number of requests is so high that the website or server is not able to cope and fails, preventing even legitimate access requests.

According to interviews conducted for this thesis, the Estonian attack caused a surge in EU interest in cyber security policy. Out of a total of 29 referable interviews, 11 stated that one of the main drivers of cyber security policy as a whole was the Estonian attack of 2007. When compared to the frequency of occurrence in interviews of the Georgian attacks of 2008 (which also alleged Russian involvement), the significance of Estonia 2007 becomes apparent. By way of comparison, the cyber-attack experienced by Georgia in 2008 was only mentioned five times in the entirety of the EU *acquis* and research interviews.

The level of interest in "Estonia 2007" is shown in Table 8-1 below, made up of the 11 direct interview references.

Table 8-1: Comments from Interview Participants on the 2007 Estonian DDoS attacks

Source	***Quotation***
(Interview, Senior Official, EC3, 2014)	[the] cyber-attack of Estonia 2007 led to establishment activity at a European Level in a more constructive manner.
(Interview, Senior Official, DG HOME, European Commission, 2014)	Shocks like 2007 and the cyber-attacks in Estonia were huge, kind of shocks that brought everyone in the Council at Member State level together, realising that cyber security was a global issue that needed a global response, or at least a European response.
(Interview, Traat and Ristikivi, 2014)	I do believe that the 2007 events were a trigger for that as well, also in the EU.
(Interview, Rönnlund, DG Connect, 2015)	There were several events. There was Estonia, there was also [the] Sony hack that had taken place. There were internet platforms that had been experiencing incidents with disruption into e-commerce so it was clear that this was having disruptive effect.
(Interview, Roehrig, EDA, 2014)	Like NATO, the EU was looking also closely on the Estonian crisis and…we saw that cyber can to a certain extent be weaponised.
(Interview, Senior Official, EEAS, 2014)	So then in this information society part there was this CIIP communication from 2009 already which was actually spurred by Estonia attacks because Estonia has organised the ministerial meeting that then was formulated into the communication in 2009.
(Interview, Helmbrecht, ENISA, 2014)	Of course if you talk about IT security you have this 2007 incident in Estonia. I think it's something where if you have such incidents it's something

	where politicians take action.
(Interview, Smith and Jones, eu-LISA, 2014)	One of the points is the cyber-attack upon Estonia. That was 2007. That was the first big one that really probably hit home to say that "God, we have to do something about these things".
(Interview, Senior Official, UK Cabinet Office, 2014)	There are cyber-attacks which intend to disable like the attack on Estonia which really was intended to disable a set of key networks.
(Interview, Pernik, ICDS, 2014)	Since [the] 2007 attacks on critical infrastructure here [in Estonia], then in Tallinn there was this first conference. Of course the EU had already before some kind of legislation for CIP but…then they focussed more on this.
(Telephone Interview, Kelam MEP, 2014)	Cyber-attacks are something opposite to privacy and then talking about cyber defences then I think that future wars or conflicts will be just played in cyberspace and this could be decisive for all of us. That's why after attacks against Estonia seven years ago the Commission has suggested to the Member states to develop their national cybersecurity strategies but even now the situation is very unsatisfactory as we have discovered because even more than half of the MS have not yet completed their national cybersecurity strategies and some have even not yet manage to ratify the Budapest convention.

The interview data demonstrates that the most immediate impact on cyber security policy was an upsurge in activity at the highest decision-making levels of the EU (Interview, Senior Official, DG HOME, European Commission, 2014). Officials at DG HOME stated that the Estonian crisis

> brought everyone in the Council [of the European Union] at Member State level together, realising that cyber security was a global issue that needed a global response, or at least a European response (Interview, Senior Official, DG HOME, European Commission, 2014).

Particular attention was paid at the time to policy concerning critical information infrastructure protection (CIIP) (Interview, Senior Official, EEAS, 2014). The DDoS attack on Estonia targeted digital information systems, disruption of which would have a serious impact on health, safety, security, and economic or social well-being. The EU therefore needed to ensure its critical digital infrastructures – both software and hardware –

were secure and could withstand large-scale, targeted attacks (European Commission, 2009a).

The Union's response was to establish CIIP policy mechanisms predicated upon the resilience of networked systems. This would be achieved through Member State and private sector co-operation, a policy standpoint which would ultimately lead to CIIP and resilience being core components of the EUCSS itself. Senior Union officials approached cyber security in a more constructive, productive manner than was previously the case (Interview, Senior Official, EC3, 2014).

The degree of importance placed on cyber security at this time is demonstrated by Rönnlund (Interview, Rönnlund, DG Connect, 2015). She argued that what was recognised at the time was that not only was the general reliance on ICT increasing exponentially, but "the likelihood and impact of incidents was getting bigger". This was especially troubling after "Estonia 2007", particularly since, according to Roehrig (Interview, Roehrig, EDA, 2014), that incident highlighted that digital technology "can to a certain extent be weaponised".

The majority of comments from the interviews point to "Estonia 2007" galvanising interest in cyber security even more effectively than the attempt to revivify that interest in the SSIS published only a year earlier (European Commission, 2006a). Officials from eu-LISA stated that the incident was a wake-up call for Union policy makers, indicating that cyber security was a serious, potent issue and that concerted action needed to be taken (Interview, Smith and Jones, eu-LISA, 2014). That action needed to do more than simply address criminal activity online or protect citizen privacy. It needed to address, or at least acknowledge, the threat of state-sponsored aggression against national communications infrastructures and the potential impact of such incidents on the EU's financial and economic viability. The result of this increased interest was a series of policy measures and instruments published after 2007 which sought to protect critical information infrastructures.

8.2.1. Policy Choice 1: Critical Information Infrastructure Protection (CIIP)

Three interview respondents stated that "Estonia 2007" spurred activity at the highest levels of EU decision-making, particularly in the area of CIIP (Interview, Senior Official, EC3, 2014; Interview, Senior Official, EEAS, 2014; Interview, Smith and Jones, eu-LISA, 2014). The EU recognised that state-on-state cyber aggression was a particularly potent

issue given the increasingly wired nature of European society and economy. Because more and more aspects of civilian and commercial life were being transferred to and operated through the digital online domain, securing the infrastructures which supported that domain was becoming ever more vital (European Commission, 2011a, p. 3). Equally important was the fact that an incident (man-made or otherwise) occurring in one Member State had the potential to create a cascading failure or domino effect affecting the whole EU communications infrastructure due to the technical interdependence of these networks. The view taken by the Union was that not only did something need to be done but it needed to be done quickly. According to senior officials at the European External Action Service (EEAS), the concentration on CIIP was a direct result of the Estonian attacks (Interview, Senior Official, EEAS, 2014). The incident highlighted the need for a pan-European capacity to ensure that information networks were protected. This was due to the dependence of an ever-increasing range of *physical* infrastructures on those information networks.

Content analyses of relevant published *acquis* from this post-2007 period support the interview evidence which points to CIIP being the preferred methodology for guarding against large-scale attacks on information systems. Triangulating the interview data with the chronology of Union *acquis* published post-2007 shows an increase in efforts to guard critical infrastructures. This pinpoints the moment that CIIP became a crucial element of EU cyber security policy. Of the 73 documents published between 2007 and 2013, 20 addressed CIIP in some way[43]. This total included two Commission Communications (European Commission, 2011a, 2009a) and three Council Conclusions (Council of The European Union, 2011a, 2011b, 2011c). A fifth Council Conclusion relating to terrorist use of cyber-attacks also referred to the importance of protecting critical information infrastructures (Council of The European Union, 2011d). This body of *acquis* literature demonstrates a high level of awareness and willingness to act on the part of the EU.

One of the core approaches undertaken by the EU to promote CIIP involved developing its role as a facilitator of co-operation, one of the five core ideational elements of the EU's cyber security discourse. This further entrenched co-operation as a *modus operandi* for cyber security. High-level co-operation and the sharing of information and intelligence regarding incidents as they occur were core elements of the EU's policy to develop and achieve CIIP. The European Forum of Member States was used as a centre facilitating high-level discussions between EU Members (Telephone Interview, Christou, University

[43] See Appendix 4 for a complete list of *acquis* relating to CIIP.

of Warwick, 2014). By 2013, the EUCSS stated that such co-operation would enable the EU to mitigate the potential cascade or domino-effect of major incidents (European Commission, 2013a, p. 16).

Although CIIP increased in significance in EU policy in this period, if the infrastructures themselves were to be able to continue functioning in the event of a sustained hack of the kind seen in Estonia, the networks and data using those networks needed to be more than just protected, they needed to be resilient.

8.2.2. Policy Choice 2: Resilience

According to Dunn Cavelty (2012a, p. 19), there are two modes of resilience in cyber security. The first of these is predicated upon ensuring that the system or network under attack can return to a pre-attack *status quo*. Handmer and Dovers (1996, p. 494) describe this as "reactive resilience", where the *status quo* is strengthened. The second strand is more flexible. It concentrates on enabling systems to adapt to the parameters of the cyber-attack to ensure that the function of the target is not impaired. For example, the function of a power station is to generate electricity. If that power station were targeted in a cyber-attack, an adaptive resilience response would mean that the priority is to continue generating power whatever the attack does, and so adapt to a new *status quo*. This is described as "proactive resilience" (Handmer and Dovers, 1996, p. 494) or "bounce back" (Herzog and Prior, 2013).

Resilience forms a substantial section of the EU's cyber security response, and for good reason. As Christou (2016, p. 4) states:

> If the EU cannot facilitate the construction of the necessary conditions for security as resilience in cyberspace in the near and long term, then there is a danger that trust and confidence in the Internet will be eroded, and that the EU will remain vulnerable to cyber-attack and, importantly, unable to react and recover in an effective way.

Trust in digital systems – another of the core ideational elements of EU cyber security policy – would almost certainly be adversely affected if the EU could not be seen to protect its own digital systems. This was of great importance for the EU. A content analysis of Union *acquis* shows that, of the 25 *acquis* instruments which specifically reference resilience, 22 come from the period 2007 to 2013, and only one was released *before* the Estonian attack. Two instances in that *acquis* demonstrate the importance placed on this concept. The first was an unusual move for the EU in this sector. In 2010, the European

Commission proposed legislation "to enhance the preparedness, security and resilience of critical information infrastructure and exchange best practice" (European Commission, 2010a, p. 6). The second was the role resilience played in relation to CIIP in the 2013 EUCSS itself.

Given the importance placed on resilience as a policy choice it is logical that this concept found its way into the EUCSS. The protection of EU infrastructures such as the Schengen information system and the asylum application database (Interview, Smith and Jones, eu-LISA, 2014) from large scale cyber-attacks is itself predicated upon the resilience of such infrastructures (European Commission, 2009a, p. 2). This is in order to ensure

> an open, secure and resilient cyberspace based on the core values of the EU such as democracy, human rights, and the rule of law, for our economies, administrations and society and for the smooth functioning of the internal market (Council of The European Union, 2013b, p. 1).

The EUCSS was not clear on precisely which mode of resilience it was seeking to achieve. At one level, the Strategy seemed to favour strengthening the *status quo* and making it resistant to change. This is evidenced in the goal of "countering cyber risks and threats" (European Commission, 2013a, p. 5) and developing tools to combat malware and botnets. At other points, the Strategy favoured more adaptive forms of resilience, as the ultimate goal of this particular measure was to support the "good functioning of the internal market" (European Commission, 2013a, p. 5).

On balance, it can be inferred that the EU favours an adaptive, bounce-back approach. The reason for this inference is that much of the focus on resilience in the EUCSS was on ensuring system functionality in the event of an incident, rather than restoration to a pre-incident state. The primary objective was to ensure that the Single Market, Internet communications and energy supply – all of which are critical physical infrastructures – continued to function unaffected. To achieve this, incidents should be reported and details shared to minimise potential damage and maximise the capacity for ICT and market systems to continue functioning (European Commission, 2013a, p. 5, 2013b, p. 6).

Although the choice of seeking to protect critical information infrastructures through ensuring their resilience to external shocks explains *how* the EU responded to the "Estonia 2007", it does not clarify *why* it responded in this manner. There are two levels to explaining this. On one level there is the acknowledged importance of ensuring physical infrastructures continue to function and serve their purpose. To do this, these

infrastructures need to be resilient. However, on a deeper level there is the question of why the EU adopted this approach to respond to a cyber security incident which bore the hallmarks of a state-sponsored act of international aggression. The answer to this deeper level is to be found in the EU's competences, and the effect of those competences on the EU's interpretation of cyber security incidents.

8.2.3. Interpreting "Estonia 2007"

As examined in Chapters 6 and 7 of this thesis, the EU's capacity to respond to state-on-state aggression or any other matter of military or defence policy was severely restricted. This is a view corroborated by officials at CERT-EU (Interview, Senior Official, CERT-EU, 2014). In 2007, the EU had no competence to act or respond to such matters in a unilateral manner. The invocation in 2007 of Article V of the NATO Charter by Estonia (irrespective of its acceptance by the NATO Council) indicated that that country's government considered the hacks an armed attack on its sovereignty. Armed attacks are, by definition, national security matters to be dealt with by an EU Member State's defence and military institutions. Such national security considerations and responses are red lines for European Union competence. As examined in Chapter 4 of this thesis, under the terms of the 1987 Single European Act, and entrenched in the 1992 Maastricht Treaty, the EU as an entity has no competence in military or defence matters. Member States retain exclusive competence in areas of national security (Zanders, 2009, p. 3).

This created something of a quandary for the EU. On the one hand the Estonian government claimed that an armed attack had taken place against its sovereignty, an area where the EU has restricted competence. On the other hand the attacks targeted national banking and government networks, disrupting access to information as well as causing failures in financial systems, albeit to a limited extent. Ensuring citizen access to information as well as the functionality and viability of financial systems was a matter of socio-economic policy. While the EU had no competence in military or defence matters, it had strong competence in socio-economic issues, particularly those affecting the Single Market. Should the digital infrastructure fail, the functionality of the Single Market would be severely compromised. The interconnected nature of digital information networks meant that an attack targeting the financial services sector of one EU Member State, such as Estonia, had the capacity to affect the entire network which underpinned critical Union infrastructures. Transposed up to the European level, therefore, an attack which could potentially disable Europe-wide banking and government data networks would have a catastrophic effect on the capacity of the EU's own economic functionality.

This quandary of how to respond to a state-backed act of cyber aggression leads to a point of particular importance in a study of the development of EU cyber security policy: the Union's CIIP and resilience-focused response to "Estonia 2007" was predicated upon a particular *interpretation* of that incident. The EU could not respond to a national security or military issue. It could, however, respond to an incident which directly, or potentially, affected the EU's financial and economic infrastructures and viability. There was the distinct possibility that this incident (or similar incidents occurring in the future) could affect EU-wide economic systems due to the potential for a cascading failure of critical digital infrastructures due to the targeting of financial networks in Estonia, and the interconnected nature of those infrastructures across Europe. The EU therefore elected to address "Estonia 2007" from this socio-economic, Single Market-oriented perspective. This afforded it great freedom of movement and policy development due to its competences in managing financial and economic policy and issues.

A specific example of this interpretation can be found in the language used by the EU to describe the 2007 Estonian incident. While the word "attack" was used in the interview responses[44] and Union *acquis*[45] to describe the incident, the term "war" or "cyber war" was never used. This is a careful and deliberate act, symptomatic of the EU's construction of a socio-economic narrative for such incidents. Were the EU to employ more military terms such as "cyber war" or "cyber warfare" in its policy response to Estonia 2007, it would be closing the door on its own capacity to act. Policy responses employing such terminology are explicitly out-with its competence. By highlighting the threat such an incident posed to the workings and ongoing functionality of the internal market, the EU converted "Estonia 2007" from a national security, defence discourse in which it has little to no competence, to a socio-economic, financial discourse in which it has far stronger competence.

This is a crucial element of the EU's overall discourse in this field, and highlights its fundamental purpose: irrespective of the nature of an incident (criminal or state-sponsored in origin), if that incident has an economic impact, then the EU can act and operate. The policy choice of resilience reflects this socio-economic perspective and construction. Rather than focus on the consequences for national security, the EU focuses on the consequences for the Single Market and European industry. The infrastructures being protected were vital to the social wellbeing of European citizens, as well as the economic functionality and viability of the Union.

[44] (Interview, Senior Official, EC3, 2014; Interview, Senior Official, EEAS, 2014; Interview, Smith and Jones, eu-LISA, 2014).
[45] (European Commission, 2009a, p. 2, 2010c, p. 16, 2010b, p. 2).

This is not simply a matter of getting round a lack of competence. It is a vitally important aspect in the understanding of EU cyber security policy over the course of the 28-year timescape. Over the course of that timescape, the EU constructed a socio-economic discourse for cyber security. This discourse began in 1985 with the concentration on the burgeoning ICT sector as an area where economic growth and employment could be stimulated. This policy choice set the precedent – the path dependence – for a focus on socio-economic matters in ICT. Such a standpoint was inadvertently entrenched by the provisions of the SEA in 1987, which stipulated that the EU could not become involved in national security matters but only in the political and economic aspects of security. This restriction was not specifically intended to be applied to cyber issues. The impact on cyber security of these Treaty restrictions was a functional spillover (Haas, 1958, p. 297) of a desire on the part of Member States in the 1980s to ensure that national security remains their remit alone.

Twenty years later, by 2007, these restrictions in competence had created a particular narrative of cyber security which influenced the manner in which the EU addressed major historical cyber events such as "Estonia 2007". As explained in Chapter 4 the competences restrict the Union to specific areas of policy, but the remit and capacity of the EU to act *within* those areas is quite extensive. By approaching the "Estonia 2007" from a socio-economic perspective, the EU afforded itself a significant capacity to act. This capacity is similar to its response to the financial crisis of the late 1980s, which sparked the original interest of the EU in ICT.

Although this socio-economic narrative was effectively applied to the EU's response to the cyber-attack on Estonia, that narrative would be tested in the Union's response to the second external, catalytic driver of cyber security policy-making: the global financial crisis of 2008. Union responses to this crisis bore striking similarities to the actions undertaken in 1985. In response to a major international financial downturn, the EU chose to focus on supporting the information sector to stimulate growth and employment.

8.3. Crisis 2 – The 2008 Financial Crisis

The content analysis of *acquis* employed to identify and triangulate data demonstrating the influence of "Estonia 2007" on EU cyber security policy also yielded evidence of a second event which fuelled policy-making in a similar manner: the commencement of the global financial crisis of 2008. Although the crisis originated in the US sub-prime mortgage market (Coffee Jr, 2009, p. 6; Schwartz, 2009, pp. 20–22; Shiller, 2012), EU *acquis* from

this period demonstrated that it had a major impact on the constituent national economies of the EU, and as a result on the Union's economy as a whole. Finding the EU in a major recession, the European Council sought means to exit the crisis (European Council, 2008, p. 3).

An examination of the EU's policy response highlights striking similarities to that of the mid-1980s, responses examined in Chapter 6. Any and all means to exit a financial downturn were sought and exploited. As with the initiation of the Single Market in 1985, in 2008 the ICT sector was singled out for specific attention. The case will be made in this section of this chapter, therefore, that the EU's policy in the immediate aftermath of 2008 was almost a carbon copy of the policies of 1985. Where there are differences, they are to be found in the admixture of cyber security matters – cyber-crime, privacy, data integrity – resulting from the development of cyber security policy over the course of the years between the financial crises. Part of this policy response was securing the digital domain from the shocks of major financial turmoil, i.e. the EU's digital domain needed to be resilient not just to external attacks but also to economic fluctuations.

The financial crisis of 2008 has been called the biggest financial and economic crisis in 80 years. It began in the sub-prime sector of the US mortgage market (Carmassi et al., 2009, pp. 977–978; Melvin and Taylor, 2009, p. 1243). Due to ever-increasing property prices, households were encouraged to borrow more to buy property with little regard to the ability to pay off the debt. The bursting of this credit bubble set in train a cascading series of failures caused by systemic weaknesses in financial infrastructures (Crotty, 2009, p. 564). The "New Financial Architecture" of post-1980s deregulation led to financial markets with very loose government or regulatory oversight. As a result, insufficient safeguards were in place to prevent financial institutions overextending themselves to the extent that they would eventually need substantial government bailouts. Exposure to such risks led to crises at major investment banks including UBS and Bear Stearns and most famously led to the collapse of Lehman Brothers in 2008 (Acharya and Richardson, 2009, p. 208). This collapse caused a ripple effect throughout international economic and commercial centres which affected European financial institutions due to "dollar funding shortages" (Baba and Packer, 2009, p. 1351).

To respond to the crisis in the EU certain industrial sectors were identified where stimuli would be established to increase economic growth and employment. In a move of striking similarity to that of 1985, the digital domain was specifically earmarked for attention

(European Council, 2010, p. 2,4). As a result a "Digital Agenda for Europe" was initiated (European Commission, 2010c). This was a programme intended to increase uptake of digital technology in all sectors of society – political, social and economic – and transform the EU into a knowledge-based economy. Its primary aim was "to deliver sustainable economic and social benefits from a digital single market based on fast and ultra-fast Internet and interoperable applications" (European Commission, 2010c, p. 2). Such measures were designed to get European economies back on track. The European Commission posited a "virtuous circle" for this digital economy, which interlinked core areas such as tackling cyber-crime, promoting research and development and increasing provision of borderless services (European Commission, 2010c, p. 4).

When compared to "Estonia 2007", the financial crisis was not a matter of direct, clear policy relevance to cyber security. However, given the narrative employed by the EU to tackle large-scale cyber-attacks – a socio-economic approach focusing on securing infrastructures vital to the economic wellbeing of the Union – the link becomes apparent. A content analysis of the 73 *acquis* publications relevant to cyber security published between 2007 and 2013 identified that 16 make direct reference to the financial crisis[46] and the need to stimulate economic growth.

The reason for the link to cyber security is twofold. First, the European Union could ill-afford *not* to respond to this crisis. In its capacity as an economic entity, any issue which affected its capability to fulfil its socio-economic functions was a matter of great importance. The importance placed on this crisis is demonstrated by the response being co-ordinated at the highest levels of EU decision-making. Of the 16 documents identified relating to the financial crisis, six were European Council resolutions and three were published by the Council of the European Union. Although the two entities were part of the same institution in 2008[47], the European Council was the configuration at which heads of state and government met. This afforded that entity a greater degree of authority as an executive body of EU governance[48]. According to an official from the former DG MARKT, this demonstrated the importance placed by the EU's highest-level actors on the financial crisis. It also greatly increased the speed at which action could be taken (Interview, Senior Official, DG MARKT, European Commission, 2014). EU decision-

[46] See Appendix 5 for the list of *acquis* which cite the 2008 financial crisis. While the evidence for the influence of the "Estonia 2007" came primarily from interview data, the evidence for the influence of the financial crisis is drawn from the *acquis* itself.
[47] Until the entry into force of the Treaty of Lisbon
[48] But without the legislative powers of the Council of the European Union.

making is notoriously slow. It takes years for proposals for action to be implemented (Interview, Senior Official, EC3, 2014). However, if the situation demands, the European Council can *require* that action be taken and decisions implemented swiftly by the other institutions (Interview, Senior Official, DG MARKT, European Commission, 2014)[49]. While it does not have any legislative capacity, the European Council has a significant amount of normative power at its disposal which can be called upon as the situation arises to require that measures be undertaken in an emergency situation. The European Council summit meetings of 2015 and 2016 in response to the Syrian refugee crisis also serve as an example of the European Council exercising normative power to address a socio-economic concern.

It is therefore significant that the measures proposed by the European Council from 2008 included ones that had a direct influence on cyber security policy. The European Council sought any and all means available to exit the financial crisis, as was the case in the 1980s. As indicated above, the main thrust of the policy response to achieve this can be found in the Digital Agenda. This was a flagship EU policy, and specifically targeted ICT and the digital domain. In its Communication of 2010 launching the Digital Agenda, the European Commission promoted small and medium sized enterprises (SMEs) as the foundations for this economic growth (European Commission, 2010c, p. 6,27).

These policies were remarkably similar to those of the Commission's 1985 Communication and the Bangemann Report of 1994. Both of these documents earmarked the ICT industry as a sector where specific Union support would generate economic growth and boost employment (Bangemann, 1994, p. 10; European Commission, 1985, p. 20). The similarity of policy options is significant as it implies a powerful path dependency when responding to financial crises. There appears to be a stock set of policy options with regard to ICT to which the EU returns when faced with a financial crisis: promote digital commerce in SMEs and encourage private sector investment to stimulate national and pan-European economic growth and employment. The sum total of measures proposed reflects the desire on the part of the EU for greater co-operation between all sectors of society affected by the economic downturn. This reinforces the continuity of co-operation as a core ideational element in EU cyber security and a repetition of policies of the late 1980s and early 1990s: closer co-operation in core areas such as ICT to capitalise on the increasing use of digital technology.

[49] In the case of the financial crisis the decision was quickly taken to establish a Eurozone banking union. Had this been proposed by the Commission out-with a time of crisis, this would have taken years to develop and implement if it were implemented at all.

While the economic motivations fuelling Union policy in ICT and networked technology had remained largely static over the preceding 20 years, by 2008 part of that policy included consideration of issues such as online criminal activity (Council of The European Union, 2009; European Commission, 2012b), the protection of minors when online (Council of The European Union, 2012, 2011d, European Commission, 2012c, p. 196, 2011b, 2011c, p. 566) and the protection of digital privacy in general (European Parliament & Council of the European Union, 2009). These criminal justice considerations were previously considered separate to economic matters. This was because they had come about as separate policy issues as the EU's reliance on digital technology evolved and developed. By 2008 these issues were considered as part-and-parcel of a wider economic policy to utilise the digital domain to maximise growth.

As with the EU's response to "Estonia 2007", the key methodological approach to addressing these concerns was once again to achieve resilience through co-operation. Just as systems and networks had to be resilient to attacks, national and European economies also needed to be resilient to more abstract financial shocks such as the collapse of Lehmann Bros., criminal activity such as malicious hacks of information systems (European Commission, 2007a, p. 2) or breaches of data protection (Council of The European Union, 2007, p. 2). Given the apparent increase in cyber-crime and the lack of trust in the digital domain, the need to establish, maintain and develop trust in cyberspace was considered a requirement (Council of The European Union, 2011d, p. 3) given the dual crises of "Estonia 2007" and the financial crisis of 2008.

The nature of the EU's cyber security discourse, and the background to that discourse, shows a second way the financial crisis influenced policy. As examined in the previous section of this chapter, the EU's response to the Estonian attacks of 2007 was dictated not by national security or military-defence concerns, but by the EU interpreting that incident as a socio-economic threat. A cyber-attack allegedly perpetrated by another state was described in language which enabled the EU to formulate a response within the bounds of its political and economic competences. A financial crisis affecting EU economies' capacity to function needed no such construction, but fitted neatly into that narrative. By default it was part of the EU's socio-economic competences. Instead of protecting the Single Market from external malicious activity as was the case when responding to "Estonia 2007", the EU was protecting it from financial shocks. These may or may not originate outside the Union but, because of the interconnected nature of financial markets

(similar to the interconnected nature of the Internet's infrastructure) these shocks could and did cause cascading failures throughout those markets.

The EU therefore responded to both the 2007 Estonian DDoS attack and the 2008 financial crisis in similar ways. Instead of focusing on national security or defence approaches to cyber security, the EU concentrated on establishing the resilience of economic and social infrastructures to major financial shocks. The primary goal was to ensure that the Single Market continued to function in the face of both major financial and geo-political crises. To achieve both of these, resilience was the approach of choice due to the restrictions placed upon the Union by its competences.

8.3.1. The Influence of External Crises: Policy Continuation vs Policy Change

The external events of 2007 and 2008 had a substantial influence on the development of EU cyber security policy. The cyber-attacks on Estonia in 2007 galvanised political interest in the field throughout the world and have since featured regularly in cyber security literature (Christou, 2016; Dunn Cavelty, 2012b; Gaycken, 2012, 2011; Rid, 2013; Valeriano and Maness, 2015)[50]. Interview data analysed for this thesis demonstrates that the incident spurred political interest at the highest levels of EU governance. This resulted in a concentration on critical information infrastructure protection (CIIP) and resilience. The thinking was that digital networks must continue to be serviceable due to the ever-increasing number of other infrastructures which depend on them. The aim was to ensure that the Single Market and the wider economic viability of the EU as a whole would continue in the event of a major cyber-attack.

One of those secondary infrastructures was the financial sector itself. The 2008 financial crisis demonstrated that economic systems needed to be resilient not just to man-made malicious incidents, but to fluctuations originating in other financial centres. This revivified interest in the economic potential of cyberspace, in a repeat of policies implemented in the late 1980s. This was a trend which continued into the development of the EUCSS itself in 2013.

However, despite the speed at which these incidents occurred, the policy choices were not *ad hoc* responses to crises as they unfolded. Although the EU, through the European Council, moved quickly to respond to both incidents and develop policy solutions, the choices of CIIP and resilience were part of a well-established narrative of cyber security.

[50] This is a representative sample of the large corpus of cyber security literature which cites "Estonia 2007".

The choices made at previous stages of the EU's process in this field had created a political and economic policy discourse which was being consistently applied. Between 1985 and 2001 the EU sought to utilise the burgeoning ICT sector to stimulate growth, establishing an economic policy foundation for interest in this sector. Over the course of that period, illegal and harmful Internet content began to become a social problem, leading by the late 1990s to measures to combat cyber-crime and ensure citizen rights such as privacy and human dignity[51]. The Treaty-defined competences were the basis of this socio-economic discourse. These competences restricted the capacity of the EU to act in national security or military matters, in turn necessitating a focus on economics to the extent that "Estonia 2007" was re-interpreted and repackaged as an economic issue of the same sort as the financial crisis of 2008. This entrenched the EU's discourse in this field.

This continuation and entrenchment of the EU's discourse is of particular consequence to historical institutionalism, as it represents something of a paradox. As examined in Chapter 4 Section 4 of this thesis, Krasner's (1984) and Baumgartner's (2014) descriptions of punctuated equilibrium stipulate that policy choices shift from one period of stasis or inertia to another when major crises occur. The paradox for EU cyber security is that major crises which affected the development of that policy – the Estonian attacks of 2007 and the financial crisis of 2008 – did not change the EU's wider policy path. Rather, the EU's choices demonstrated a continuation and entrenchment of long-standing core policy paths of economic maximisation within a socio-economic cyber security discourse. If punctuated equilibrium seeks to explain policy *change* as the result of crises, EU cyber security policy represents an important exception to this rule. Instead of effecting a shift in policy paths from one period of stasis to another, the crises of 2007-2008 reinforced the strength of path dependent processes and are shown to be drivers of policy *continuation* rather than policy *change*.

The reason for this is to be found in the discourse constructed under the influence and restrictions of the EU's competences. These competences led, over the period of the policy-making timescape, to the development of a particular socio-economic cyber security narrative which affected the manner in which major crises were interpreted. The socio-economic construction of cyber security threats was the best, and to some extent only, way to respond to these events. The financial crisis was just that, a financial crisis. Socio-economic responses were therefore the most suitable given the issues under examination. "Estonia 2007", by contrast, was alleged to have been an act of inter-state aggression.

[51] Including the protection of children from online exploitation.

There was, however, a socio-economic impact of particular concern for the EU given the interconnected nature of information networks. The EU applied its well-established socio-economic cyber security discourse to these two incidents and developed a wide-ranging response as a result, a response still operating within the confines of Union competences. The external crises faced by the Union in this sector therefore did not alter established paths of institutional stasis. Instead, they reinforced them.

8.4. Conclusion

This chapter has shown that the effect of important exogenous events on EU cyber security policy was not to radically alter that policy, but to entrench its core elements. By 2007 the EU had established itself as an economic entity with an international presence. Faced with two major crises in as many years, the EU was required to show initiative and be creative in its responses due to its restricted competences and remits. Although the 2008 financial crisis was within its competences, the Estonian attacks a year earlier were ostensibly outside its purview. In order to be able to respond in any meaningful manner, the EU interpreted "Estonia 2007" as threats to the functionality and viability of the internal market.

The chapter also showed that the EU's preferred policy response to both of these events was to focus on resilience. Having interpreted the events as threats to the Single Market, the EU's priority was to ensure the continued functionality of digital and physical infrastructures vital to the Market's continued viability. Finally, the chapter showed that this response represented a paradox from an historical institutionalist perspective. Rather than force radical rethinks and alterations to a long-standing, socio-economic approach to cyber security, these events entrenched that approach.

It is noteworthy however, that the triggers for the events of 2007 and 2008 were both exogenous to the EU. Although they had a direct influence on EU cyber security policy, their original source was located outside the EU's geographical area[52]. Policy development need not be restricted to responses to exogenous crises, however. Internal shocks to a well-established institutional architecture are just as likely to affect policy choice. Such an internal event occurred in 2009 with the coming into force of the Treaty of Lisbon. This Treaty caused a major restructuring of the EU itself, which necessarily affected policy-making processes across the entire remit of Union competences. For cyber security, this

[52] Assuming the allegations made against Russian involvement in the Estonian attacks are eventually categorically confirmed.

restructuring ushered in a policy-making architecture amendable to a truly holistic cyber security policy.

The following chapter will therefore present evidence for two points. First, the changes initiated by the Treaty of Lisbon meant that without it, the EUCSS of 2013 would not have been possible. Nevertheless, the question remains as to whether it radically altered the EU's discourse in that field. The analysis will show that, despite ushering in a completely new policy-making architecture, the Treaty of Lisbon continued the paradoxical effects of "Estonia 2007" and the financial crisis of 2008, and further *entrenched* the EU's socio-economic cyber security discourse.

Chapter 9 | Punctuated Equilibrium Part 2: The Effect of the Treaty of Lisbon on Cyber Security Policy

9.1. Introduction

Chapter 8 examined the influence on EU cyber security policy of events which began outside the Union. This chapter will present evidence to demonstrate the influence of major events *internal* to the EU. This will be achieved through the examination of an event of singular importance in the history and development of the EU itself: the Treaty of Lisbon. The chapter will make the case that without that Treaty, the EU's *Cyber Security Strategy* (EUCSS) would not have come about. By abolishing the EU's Pillar structure and establishing provisions for mutual assistance in the face of major crises, the Treaty of Lisbon removed policy silos and reduced duplication of policy-making efforts. This enabled a holistic cyber security policy to be developed. The removal of the Maastricht Treaty's division of remits created an architecture conducive to a cross-Pillar, multi-field policy such as the EUCSS of 2013. The Lisbon Treaty is therefore an event of crucial importance to the EU's cyber security policy-making timescape. Interview and *acquis* data both point to the substantial influence it had on pushing and speeding up policy development in this field. That process ultimately culminated in the 2013 EUCSS.

In conjunction with the Estonian cyber-attack of 2007 and the financial crisis of 2008, the Treaty of Lisbon galvanised the policy development process in this field. As such these events represent major punctuation points in an otherwise path-dependent progression from 1985 to 2013. However, these three events present an historical institutionalist paradox. Under the mechanisms of punctuated equilibrium, major events and crises are punctuation points which move policy paths in new directions. The evidence presented in this chapter will demonstrate that these events had the opposite effect: rather than cause policy change, they further entrenched the Union's established socio-economic discourse and approach to cyber security issues.

The chapter will argue that the reason cyber security policies continued rather than changed was because the Treaty of Lisbon formalised *pre-existing* competences rather than afforded the EU new or expanded capabilities. This continuity of competences occurred despite the Treaty initiating fundamental change in the architecture of the EU as a whole. This meant that those policy areas heavily dependent on Union competences – such as cyber security – did not change but that policy discourses became further entrenched.

There are two observations to take from these findings. The first is of direct relevance to the research question: the institutional arrangement of Union competences led the EU to develop and continue its particular approach to cyber security. The competences lie at the heart of the Union's discourse in this field and its response to cyber security challenges. The EU's capacity to act, or more precisely, the Treaty-defined restrictions on its capacity to act, have shaped the EU's discourse in this sector and steered it towards particular socio-economic policy choices designed to ensure the resilience of the internal market. The second observation has particular implications for historical institutionalism as this entrenchment in the face of major crises represents a divergence from the mechanisms of punctuated equilibrium. This implies that punctuated equilibrium is a more flexible explanatory model as it can be used to explain policy continuity as well as policy change.

The chapter is divided into five sections. The second section provides a brief overview of the primary changes to the structure of the EU brought about by the Treaty of Lisbon itself. The third section provides a detailed examination of how the removal of the Pillars of the Maastricht system enabled the development of the EUCSS. The fourth section examines the paradox of the Treaty's lack of influence on the EU's cyber security discourse due to the continuous nature of Union competences. The fifth section concludes the chapter.

9.2. The Effects of the Treaty of Lisbon: Restructuring the EU's policy-making architecture

On 1 December 2009 the Treaty of Lisbon came into force[53]. In an effort to create a more effective and efficient policy-making and policy-implementing structure, the Treaty initiated a number of radical changes in the way the EU was constructed. At its core was the repackaging of the Treaties of Amsterdam and Maastricht into the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). The aim of this repackaging was to ensure coherence and comprehensibility as well as increase effectiveness in policy development and implementation across the array of fields in which the EU was involved (Dinan, 2010, p. 154; Verdun, 2013, p. 1131). In addition, the European Parliament was placed on an equal footing with the Council of the European Union by being granted co-decision powers on legislation (Craig, 2008, p. 13). The European Council, until this point a corollary to the Council of the European Union, was established as a "formal institution" in its own right (Craig, 2008, p. 9). Article 9 of the

[53] It was signed, however, on 13 December 2007. It is not the aim of this chapter or this thesis to enter into a lengthy examination of the Treaty of Lisbon, its developmental history or its impact on the wider EU in general. Such analyses have been conducted elsewhere (Craig, 2010, 2008; Dinan, 2010; Verdun, 2013; Weatherill, 2014).

Treaty established the seven formal institutions of the EU as the European Council, the European Commission, the Council of the European Union, the European Parliament, the European Central Bank, the Court of Justice and the Court of Auditors (European Union, 2007, p. 16).

The Treaty also codified the exclusive, shared and supporting competences of the Union, as well as specifying the various policy areas in which each competence was employed (European Union, 2007, pp. 46–48). The EU enjoyed exclusive competence in, *inter alia*, managing the internal customs union, establishing the competition rules necessary for the functioning of the internal market, and "monetary policy for the Member States whose currency is the Euro" (European Union, 2007, p. 47). In matters relating to social policy, transport and the internal market, the EU shared competence with the Member States. While it did not enjoy sole management of the internal market, sharing competence in this field placed the EU on a level footing with Member States in terms of initiating policy. In the fields of culture, tourism, education and sport, the EU had "to carry out actions to support, co-ordinate or supplement the actions of the Member States" (European Union, 2007, p. 48). This was the weakest form of competence.

In the fields of foreign affairs and security policy the role of the High Representative of the Union for Foreign Affairs and Security Policy (HR) was expanded so as to represent the EU as a whole on the international stage. The HR was to be assisted in the fulfilment of Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CDSP) goals by a new European External Action Service (EEAS). The EEAS would also serve as a *de facto* diplomatic service of the EU. This was to be achieved by

> co-operation with the diplomatic services of the Member States and shall comprise officials from relevant departments of the General Secretariat of the Council and of the Commission as well as staff seconded from national diplomatic services of the Member States (European Union, 2007, p. 27)

In addition the European Defence Agency (EDA) was officially confirmed as a formal EU body (Howorth, 2013, p. 13).

Demonstrating the importance placed on the field of cyber security as a whole, "computer crime" was specifically mentioned as an issue and area requiring co-operation in Article 69(b) of the Treaty (European Union, 2007, p. 65). It is a field of crucial significance to the stability and viability of the internal market due to the nature of the security challenges involved. In terms of practical solutions to those challenges, however, the most significant

impact of the Treaty of Lisbon on cyber security policy was the abolition of the Maastricht Treaty's pillar structure.

9.3. Removing the Maastricht Pillars

As examined in Chapter 6 Section 3.2, under the policy-making structure instituted by the 1992 Treaty of Maastricht key aspects of cyber security policy were handled under different "Pillars". These Pillars covered different policy areas and were subject to different decision-making procedures and levels of competence. The impact of this system on cyber security policy-making was the development of a highly fragmented library of *acquis* comprising different policy and legislative instruments. There was no over-arching strategy addressing all elements of cyber security. By 2002 it was recognised by the European Council that this caused a certain degree of duplication due to the fact that cyber issues crossed not only geo-political boundaries, but also policy areas (Council of The European Union, 2002a, p. 4). Due to the existence of the Pillars, a truly holistic cyber security policy was not possible.

Under the terms of the Lisbon Treaty creating a single legal personality for the EU, the Pillar structure was abolished. This created a single, streamlined and more efficient policy-making architecture. For the first time in the EU's history functionaries and officials from agencies and Commission Directorates-General (DGs) operating across what used to be distinct and functionally separate areas of the Communities, judicial co-operation and foreign and security policy were able to work together in a formal capacity (Interview, Helmbrecht, ENISA, 2014; Interview, Senior Official, EEAS, 2014; Telephone Interview, Kelam MEP, 2014). This in turn created a policy-making system conducive to the development of a holistic cyber security policy, the result of which was the EUCSS (Interview, Senior Official, EEAS, 2014).

This change more than any other enabled more collaborative work to be done in cyber security and eliminated the risk of duplication of efforts or a lack of awareness between the Commission DGs. Activities which had been carried out in isolation were more joined-up after 2009 (Interview, Purser, ENISA, 2014). In the field of cyber-crime, for example, officials previously working under the Justice and Home Affairs Pillar of judicial co-operation (Pillar 2) were able to work under Pillar 1 policy development and decision-making processes. This afforded the Commission two important capabilities. Under Pillar 1, the Commission had the right of initiative. This meant that it could propose policy or legislative instruments wherever it saw a need or gap. By extending this right to what used

to be Pillar 3 (Justice and Home Affairs) DG HOME, and thereby the Commission itself, was afforded this right of initiative in the field of cyber-crime (Interview, Senior Official, DG HOME, European Commission, 2014). The effect was to enable more judicial and policing co-operation (Interview, Smith and Jones, eu-LISA, 2014), particularly at Europol.

9.3.1. Promoting Co-operation

By 2009 the high-tech crime centre established at Europol had developed into an established pan-European hub in its own right (Interview, Senior Official, EC3, 2014). It had a multiplier effect, able to direct, pool and co-ordinate resources to tackle cyber-crime across all the Member States. This removed the requirement for individual Member State capacity-building or bilateral arrangements. Before 2009, however, the Commission did not have the ability to initiate policy or legislative proposals to support the EC3 in its activities. With the entry into force of the Treaty of Lisbon, it could. The Commission also now had enforcement capacities in this field. It could ensure that all elements of the relevant cyber-crime *acquis* were implemented by all Member States. The Commission could also launch infringement procedures were this implementation not undertaken (Interview, Senior Official, DG HOME, European Commission, 2014). These two features highlight a dramatic increase in the capacity of the EU to act in the field of cyber-crime, an important ideational element of the Union's wider cyber security policy throughout the entire 28-year timescape.

This capacity for joint working had two impacts on cyber security policy far beyond tackling cyber-crime. According to officials at the EDA and eu-LISA the EU was able to look outward in its policy and address external cyber issues in a way that previously it could not (Interview, Roehrig, EDA, 2014; Interview, Smith and Jones, eu-LISA, 2014). This enabled the EU to address incidents such a major cyber-attack originating outside the EU – as was the case in Estonia in 2007 – but remain within its competences. As Smith and Jones from eu-LISA stated (Interview, Smith and Jones, eu-LISA, 2014), the removal of the Pillar system coupled with the initiation of the EEAS enabled the EU as a whole to establish the coherence of policy that was missing before 2009. This in turn enabled it to address the fragmentation of that policy area, particularly in crisis management under Article 222 of the revised Treaty on the Functioning of the European Union (TFEU). This additional article is known as the Solidarity Clause (European Union, 2009b, p. 148)[54].

[54] See Appendix 13 for the full Clause.

Two interviews mentioned this clause as being of specific relevance to cyber security, in particular the capacity to deal with major cyber-attacks (Interview, Roehrig, EDA, 2014; Interview, Smith and Jones, eu-LISA, 2014). Both the EDA and eu-LISA cite Article 222 as an important addition to the capacity of the EU to respond to major cyber incidents. Described by Roehrig (Interview, Roehrig, EDA, 2014) as a clause sitting between Articles IV and V of the NATO Treaty, it states that the Union and its Member States shall act "jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster". The clause cannot be compared directly to Article V of the NATO Treaty which stipulates that an attack on one member is an attack on all, simply due to the fact that the EU is not a military organisation. Instead, the Solidarity Clause is a commitment to mutual assistance in the event of a disaster, thus cementing co-operation as an ideational driver. Cyber-attacks are not explicitly mentioned as causes which would necessitate the activation of this clause. However, it is inferred by officials from eu-LISA that such an incident could be of significant scale to constitute a man-made disaster. As Smith and Jones state:

> It's a clause that a Member State can call upon in case of need. What that case of need might be depends upon the Member State that might [call up] actions but at least within certain documents cyber-attack is one of the examples given where solidarity would be called on (Interview, Smith and Jones, eu-LISA, 2014).

Although Roehrig from the EDA and Smith and Jones from eu-LISA specifically mentioned the presence of the Solidarity Clause as being of importance and relevance to EU cyber security policy, these were only two interviews out of the total number of 30 referable interviews conducted. As a result it is unwise to infer too great an influence of that clause on the wider narrative in this field. Nevertheless, such a commitment to mutual assistance represents a significant step-change in EU crisis management in general. The clause stipulates that Member States are to render such assistance as is required by the victim state and that "the Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States" (European Union, 2009b, p. 148). When applied to an analysis of the DDoS attack against Estonia in 2007, and the paralysing effect that incident had on that country's digital infrastructures, such a clause presents a significant capacity for action. It also formalises in Treaty provisions an important co-ordinating role for the EU itself. The clause states that the Council of the European Union will be the mechanism through which Member State assistance efforts would be co-ordinated. This codified in Treaty provisions the EU's role as a facilitator of

co-operation during crisis situations, inferred by eu-LISA to include cyber-attacks (Interview, Smith and Jones, eu-LISA, 2014).

The Treaty of Lisbon therefore provided the EU a formal capacity in crisis management as an entity in its own right. While not granting the EU any executive powers, it enabled it to co-ordinate the extensive resources of its Member States, including military capabilities. Care must be taken at this point not to overemphasise the significance of this. As stated above, of the interviews carried out only two state the relevance of the Solidarity Clause to EU cyber security policy. Nevertheless, just as it would be imprudent to overstate the significance of this point, it would be a mistake to ignore the potential applicability of the clause to incidents such as "Estonia 2007", should they be repeated in the future.

The result of the removal of the Pillars and establishment of a new capacity for joint-working led to a second influence of the Treaty of Lisbon on EU cyber security policy-making. Officials from Commission DGs HOME and Connect, and the new External Action Service, could for the first time come together in an official capacity to develop a strategy document encompassing all elements of EU cyber security *acquis*. The result of this joint working was the *Cyber Security Strategy of the EU - An Open, Safe and Secure Cyberspace* (Interview, Senior Official, EEAS, 2014; Interview, Smith and Jones, eu-LISA, 2014). According to Tunne Kelam MEP this was made possible by the new framework of the Treaty of Lisbon (Telephone Interview, Kelam MEP, 2014). At the time this was unique, for it represented the first time all three former Pillars were present in the development of a single policy (Interview, Senior Official, EEAS, 2014). DG Connect, prior to 2009, fell under Pillar 1. The EEAS was the new agency initiated by the Treaty of Lisbon responsible for managing and developing the CFSP, the former Pillar 2. DG HOME had been granted the right of initiative in criminal justice affairs which had previously fallen under the aegis of co-operation in judicial affairs, or Pillar 3. The new, streamlined EU resulting from the Treaty of Lisbon enabled this unprecedented level of joint working not just between overlapping policy areas but between the Commission's departments themselves. This resolved the problem of a silo mentality resulting from the pre-2009 Pillar system (Interview, Helmbrecht, ENISA, 2014). This new architecture and combination of Pillar influences can be identified in the EUCSS itself.

9.3.2. Combining Pillars in the EUCSS

The EUCSS presented a "vision" of cyber security based around five strategic priorities which address the challenges of living and working in the 21st century. Taken directly from that document, these priorities are:

- "Achieving cyber resilience;
- Drastically reducing cyber-crime;
- Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP) ;
- Developing the industrial and technological resources for cyber security;
- Establishing a coherent international cyberspace policy for the European Union and promote core EU values" (European Commission, 2013a, pp. 4–5)

Of these five strategic goals, three are direct representations of the pre-2009 Pillars: the Communities, CFSP, and Judicial Co-operation.

Prior to 2009, the strategic goal of drastically reducing cyber-crime was developed under the aegis of Pillar 3 as it was a part of the field of police and judicial co-operation. There are a number methods expounded in the EUCSS by which the EU sought to achieve this goal. Most were centred on facilitating co-operation and information-sharing. Agencies such as Europol and Eurojust were tasked with working more closely together "in order to increase their effectiveness in combating cyber-crime, in accordance with their respective mandates and competence" (European Commission, 2013a, p. 11). The EUCSS also recommends the ratification of the Council of Europe's 2001 Convention on Cyber Crime (European Commission, 2013a, p. 9), better known as the Budapest Convention[55]. The EUCSS also stipulates that the EU would support Member States in the establishment of their own national cyber-crime units.

These actions and policies are reminiscent of the pre-Lisbon intergovernmental approach to policing and judicial co-operation. The EU itself did not seek to establish or set up specific judicial or technical measures to tackle cyber-crime. Instead it advocated better use of current capabilities in Member States, and promoted better co-ordination, through the EU, of those capabilities. These included the more effective application of existing legislation and instruments, including the Budapest Convention, and certain of the EU's own instruments on tackling online child exploitation (European Parliament & Council of The European Union, 2011). This position, of facilitating co-operation, is reminiscent of the

[55] To date, this is the only international treaty in the field of cyber security (Council of Europe, 2001).

core function of Eurojust within Pillar 2 *prior* to the entry into force of the Treaty of Lisbon. Before 2009 Eurojust's function was to

> increase the exchange of information between the interested parties, facilitate and strengthen co-operation between national authorities and Eurojust, and strengthen and establish relationships with partners and third States (Eurojust, n.d.).

This afforded it the same supporting role as Europol, i.e. co-ordinating information-sharing from the Member States' national prosecuting offices but without executive powers of its own.

That supporting and facilitative role could, in certain circumstances, translate into specific action in providing analytical and operational support to Member States. This could be provided via the EU's operational agencies such as Eurojust and Europol. As set out in Chapter 7 Section 2.1, Europol has no executive powers. However, while it cannot make arrests, it can call upon a great deal of expertise (Interview, Senior Official, Europol, 2014). A senior official from the EC3 cited the example of a recent major incident where the local Member State police did not have the forensic capabilities to analyse a crime scene. In this instance Europol provided direct assistance in the form of forensic and analytical experts. The results and findings were given to the Member State police who carried out any resulting arrests (Interview, Senior Official, EC3, 2014). As the official described, Europol provides the detailed analysis of the crime scene or other data, but it is the Member State police forces who took executive action (Interview, Senior Official, Europol, 2014). While not specifically a cyber-crime issue, the point of this example is that the forensic experts were Europol agents, rather than Member State police officers. Europol was facilitating the sharing of expertise and experience in a situation where the local police services did not have the required resources. This enabled the EU to fulfil a role as an advice and expertise broker and co-ordinator of co-operation.

That co-ordinating function is also brought to bear in the third of the five key strategic goals, developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP) (European Commission, 2013a, p. 5,11). In this policy area, the EU is seeking to develop cyber defence capabilities within the framework of the CSDP (European Commission, 2013a, p. 11). At face value, this goal reads like a mandate for developing Union cyber warfare capabilities, something at which most Member States would baulk. Closer examination, however, reveals this not to be the case. The cyber defence section of the EUCSS is the weakest, most under-developed aspect of that

document. At half a page long, it is the shortest section and contains none of the direct supporting action of, for example, that advocated in tackling cyber-crime. It contains no references to possible legislative instruments to assist Member States or require co-operation. ENISA and Europol do not feature as the agencies operationalising this facilitative role in this particular area. Reflecting the limited capacity for action in the pre-Lisbon CFSP Pillar 2, this section once again advocates co-operation between interested parties and is assuming the role of *facilitator* between those parties, rather than advocating, for example, the development of specific, EU cyber warfare tools.

To achieve this co-operation the High Representative of the Union for Foreign Affairs and Security Policy (HR) and the European Defence Agency (EDA) are tasked with engaging with partners such as NATO to ensure that there is no overlap of responsibilities or duplication of efforts (European Commission, 2013a, pp. 15–16). This desire to avoid duplication further distances the EU from specific action in cyber security. This continues the arms-length approach begun in 2006. While the Union can pass legislation enforcing co-operation in the areas of resilience and cyber-crime, the EU is effectively leaving European cyber defence to NATO.

There are two reasons for this. The first is that NATO, as a military alliance, is best placed to deal with military-defence issues in cyberspace. It is developing policy and capability within the bounds of its membership Charter, utilising the tools made available by its signatory states (Interview, Traat and Ristikivi, 2014). In addition, it has its own research centres such as the Co-operative Cyber Defence Centre of Excellence (CCDCOE) based in Tallinn, Estonia. To have the EU also engaging in such activities, particularly when a number of Members of NATO are also Member States of the EU, may lead to an inefficient duplication of efforts (Interview, de Vries, National Cyber Security Centre of the Netherlands, 2014; Interview, Ottis, Tallinn University of Technology, 2014). As Smith and Jones of eu-LISA state, "the intention even from a pure strategic point of view shouldn't be to do the same [thing if] someone else is doing it already" (Interview, Smith and Jones, eu-LISA, 2014).

The second reason is that the EU has very restricted competence in defence matters. This is a clear throw-back to the pre-2009 Pillar of the CFSP. As examined in Chapter 4 Section 2.1, the competences of the EU define in what policy area and to what extent the EU may become involved. Foreign and security policy is an area of highly regulated EU action and consequently weak Union competence (Craig, 2010, p. 183). So strong and

focussed is Member State government oversight and control in this field that one interviewee remarked that the European Parliament's Security and Defence Committee is a "toothless tiger" due to its lack of direct, discernible impact (Interview, Senior Official, European Union, 2014). Despite its inclusion in the EUCSS, cyber defence retains the restrictions placed on Union defence policy established under the pre-Lisbon Pillar system demonstrating continuity of competences.

While action in cyber defence is minimal, EU involvement in the fourth strategic goal, developing industrial and technological resources for cyber security, is far more forthright, dynamic and assertive. This reflects and continues the patterns of policy-making in Pillar 1 – the Communities – established prior to 2009. While the Union as an actor is weak in terms of cyber defence, it comes into its own in developing industrial and technological resources, particularly where these impact on the development and sustainability of the internal market.

According to the EUCSS, the central goal of EU policy in this area is to establish an internal market for European-manufactured security products and services. This is to be fostered by research and development assisted by a number of initiatives including the Horizon 2020 programme (European Commission, 2013a, pp. 12–14). This was a wide-ranging initiative intended to strengthen the Union's "excellence in science", foster industrial leadership to support business and tackle societal change such as "migration, integration, demographic change, the ageing society and disability" (European Parliament and Council of The European Union, 2013b, p. 105,163). The thinking behind this is not purely commercial. It reflects the EU's desire to ensure the on-going economic and functional viability of the Single Market by ensuring competitiveness (European Parliament and Council of The European Union, 2013b, p. 167). In order to ensure the security of systems and infrastructure, as well as engender trust in that infrastructure, the entire supply chain for building and maintaining ICT networks, from manufacturing silicon chips to laying physical cables, must be secure. The EU recognised that European users depended largely on non-European solutions for cyber protection (Olesen, 2016, p. 261). European products and technical expertise would contribute to a more dynamic and secure Digital Single Market.

The US recently set a precedent for this digital autarky by banning the use of Chinese-manufactured components in any American ICT infrastructure systems[56]. This followed

[56] In this particular example those made by Huawei.

allegations that Chinese software and hardware companies were installing "backdoors"[57] at the behest of the government in Beijing thereby enabling the Chinese military to access these systems (Interview, Senior Official, UK Cabinet Office, 2014). While the allegations were strenuously denied, the US took no chances. The EU sought to develop a similar system. It was, according to the EUCSS, acutely aware that European ICT infrastructures rely heavily not only on private operators but on extra-territorial, 3rd-country manufacturers for its components and software (European Commission, 2013a, p. 12). This has the potential to weaken the information infrastructure on which so many other physical systems rely.

The approach the EU took to resolve this problem reflected patterns of policy developed under the pre-Lisbon Communities Pillar: incentivising the private sector, fostering co-operation and establishing minimum standards, in this case through a voluntary certification scheme. Because this is a policy area focused on the Single Market, the EU, and in particular the Commission, could flex its muscles and be more proactive. It sought to establish a platform for solutions to incentivise private sector industry to build security into their products (European Commission, 2013a, p. 12). Considering security as integral to product design, and indeed to infrastructure design itself, was argued by Ilves (Interview, Ilves, Govt. of Estonia, 2014) and McGraw (McGraw, 2013) as a better methodology than considering security as an additional layer or "bolt on". European standardisation bodies, in particular the European Standardisation Organisation and the Cybersecurity Co-ordination Group (European Commission, 2013a, p. 13), were tasked with developing certification programmes under the Smart Grids Standard and ensuring private sector engagement. Funds from the Horizon 2020 project were also earmarked for research and development programmes for trustworthy ICT systems to be used in the fight against cyber-crime (European Commission, 2013a, p. 14). All these measures were intended to reduce the EU's reliance on non-EU technology which may or may not be compromised.

The strategic aims of the EUCSS demonstrated a combination and continuation of core elements of the pre-Lisbon Pillar system. Tackling cyber-crime, part of police and judicial co-operation, was a specific goal of the EU. This was positioned alongside ensuring a lack of over-lap with NATO capabilities and policies in cyber defence, a clear remit of the former CFSP Pillar. Both of these "strategic priorities" were intended to ensure the ongoing economic and functional viability of the Single Market and of the EU itself, a

[57] Backdoors are intentionally installed software and hardware loopholes enabling unauthorised access.

policy area of the former Pillar 1, the Communities. Such a combination of Pillar remits, however, would not have come about prior to 2009. The entry into force of the Treaty of Lisbon, and its abolition of the Pillars themselves, enabled a level of joint-working and collective policy-making not previously possible. This had important consequences for EU cyber security policy-making. The nature of cyber security is such that policy remits and divisions are effectively irrelevant. The threats and risks to cyberspace affect all aspects of policy-making regardless of abstract political divisions such as the Maastricht Pillars. Those Pillars were, however, hampering efforts to create an effective policy solution because it was not possible to develop a strategy which encompassed *all* areas of risk. The Treaty of Lisbon removed those obstacles and enabled a holistic policy approach, the EUCSS, to be developed.

9.4. The Impact of the Treaty of Lisbon on EU Cyber Security

The new architecture of the EU initiated by the Treaty of Lisbon was an important milestone in the EU's cyber security policy-making timescape. Of particular influence were the removal of the Pillar system and the expansion of the Commission's right of initiative. Without this structural change the EUCSS could not have been developed. The removal of the Pillar structure enabled DGs separated by distinct policy remits to work together to reduce the duplication of efforts and develop a cohesive approach to cyber security. The Treaty also created the EEAS, which brought foreign and security policy concerns to the cyber security policy-making process. An examination of the EUCSS itself illustrates the presence of policy initiatives which would have been developed under separate Pillars: initiatives in tackling cyber-crime (Pillar 3); developing cyber defence co-ordination (Pillar 2); and protecting the internal market (Pillar 1).

Avoiding duplication of efforts was a key element of the Treaty of Lisbon. In reforming the treaties on which the EU was founded its goal was achieving simplicity (Christiansen and Dobbels, 2013, p. 1164). The changes it ushered in were intended to tackle perceived deficiencies in effectiveness, efficiency and democratic accountability. It sought to streamline processes and responsibilities. In doing so it achieved, in many respects, a more coherent and comprehensible European Union. The Treaty of Lisbon was therefore what Pierson (1995, p. 458) labelled a "positive-sum" effort, one designed to sort out responsibilities within an architecture in a manner that better meets the needs of all actors involved.

Although the goals of streamlining policy- and decision-making were not directed at any specific policy area, they can most clearly be seen in the field of cyber security. By 2009, cyber security policy had a 24-year heritage in the EU with the result being a fragmented and diverse library of differing legislative and policy instruments. This included white and green papers, strategy documents, formal legislation, European Council pronouncements and conclusions of the Council of the European Union. All of these were produced under differing decision-making and developmental patterns within the policy debates of those actors. Creating additional fragmentation was the division of the task of operationalising that extensive *acquis* amongst a number of specialised agencies such as ENISA, the EC3 and CERT-EU. By abolishing the old Pillar system, offices that were not able to work together could now do so under the EU's new institutional structure (Interview, Senior Official, DG HOME, European Commission, 2014). As a result, a single strategic approach to cyber security was developed which encompassed the areas of the common market, critical physical and digital infrastructure, internal security and defence. Cyber security policy demonstrated the achievements of the Treaty of Lisbon in its streamlining goals. Decision-making was made more coherent, duplication was reduced and a more holistic, unified approach to a single policy area was developed.

One question remains, however. While the Treaty of Lisbon altered the architecture of the EU itself, and created an entity in which the EUCSS could develop, this does not necessarily mean that the Treaty effected any changes in the Union's underlying cyber security discourse.

9.4.1. The *Lack* of Impact of the Treaty of Lisbon on the EU's Cyber Security Discourse

While the Treaty of Lisbon ushered in major institutional change across the entirety of the EU's structure, in cyber security the *underlying* discourse remained unaltered. As examined in Chapter 5, that discourse is predicated upon five core ideational elements: economic maximisation, engendering trust in digital systems, the protection of fundamental rights, tackling cyber-crime and facilitating co-operation. Because these five elements continued to under-pin policy *after* the entry into force of the Treaty of Lisbon, it can be inferred that the EU's cyber security discourse itself not only continued unchanged, but also proved resilient to the structural changes of the Lisbon Treaty. This section of the chapter will demonstrate this continuity using evidence from *acquis* and interviews.

One of the first documents in the EU's cyber *acquis* published post-Lisbon was a Commission Communication entitled *Towards a Single Market Act for a highly competitive social market economy: 50 proposals for improving our work, business and exchanges with one another* (European Commission, 2010d). This Communication set out a series of proposals to "relaunch" the Single Market. An important component of this was the development of a *digital* single market, reflecting the importance of cyberspace for the EU's economic development (European Commission, 2010d, p. 9). The aim was to revivify political interest in the Single Market and reassure businesses of its viability in the face of the global financial crisis (European Commission, 2010d, p. 3). It was stated that the primary aim of the EU as an entity was economic and that "one big market is at the heart of the European project envisaged by the founding fathers" (European Commission, 2010d, p. 1). The purpose of this Communication was to remind citizens, businesses and politicians that economic factors lay at the heart of the EU. These included creating jobs (European Council, 2011a, p. 1) and targeting youth unemployment (European Commission, 2012c, p. 2).

Cyber security was a key element of this drive, particularly in the form of tackling counterfeiting and online piracy (European Commission, 2010d, p. 8). To promote this, the Digital Agenda for Europe was established. According to the former Bureau of European Policy Analysis (BEPA) at the Commission, "the ability to access data would be at the core of this economic growth" (Interview, Senior Official, BEPA, European Commission, 2014). This meant that digital networks and infrastructures would continue to be critical to the revitalised economy in order to secure competitiveness (European Commission, 2010e, p. 4, 2009b, p. 2; Interview, Helmbrecht, ENISA, 2014).

An important issue facing the EU in its efforts to revivify the Single Market following the hacks in 2007 and the 2008 financial crisis was a lack of trust in European economic systems. This translated into a similar lack of trust in digital technology and online commerce. A central focus of the Digital Agenda was to reverse this trend (European Commission, 2010c, p. 10) and renew confidence, not just in online transactions and communications, but by extension in the EU as a place to do business. Officials from BEPA argued that it was, for example, in Amazon's commercial interest not only to project itself as a secure and safe commercial entity, but also to be seen to be operating in a trustworthy wider economic community (Interview, Senior Official, BEPA, European Commission, 2014). This shows the continued importance of engendering trust as an ideational driver of cyber security policy.

Trust in digital systems was particularly important given the increased globalisation of markets available through online commerce. According to an EU functionary interviewed for this thesis, one third of Internet users are not confident when buying products from other countries (Interview, Senior Official, DG HOME, European Commission, 2014). The EU sought to counteract this lack of trust and promote online commercial activity. Security of transactions and security of systems were important elements of the EU's plans to engender citizen and corporate trust in digital systems post-Lisbon. A tool to achieve this was developing the resilience of economic systems and critical information infrastructures. These would address the perceived fear of hacks and cyber-attacks which was preventing users from fully engaging with the developing Digital Single Market (European Commission, 2009a, p. 5).

One cause of this reluctance to use digital online media for commercial transactions, certainly from a private citizen's perspective, was the fear of personal financial or identity data being lost or compromised. Several interviewees stated that private citizens are more aware of their right to privacy and the capacity for their personal communications and transactions to be monitored due to the exposure by Edward Snowden of details of mass surveillance of communications by government security agencies (Interview, Senior Official, European Union, 2014; Interview, Senior Official, UK Cabinet Office, 2014). Labelled "Snowden Fallout" by the UK's Department of Business, Information and Skills (Interview, Senior Official, BIS UK, 2014), there was an increased awareness of the need for personal data protection. This protection was needed not just from criminal actors seeking such digital information for personal gain, but also protection from overzealous security services. This was a form of mission creep warned against by Deibert (2009, p. 327). Data protection and anti-surveillance policies became a politicized issue after the Treaty of Lisbon. This is evidenced by the Green party bloc in the European Parliament pushing for greater citizen protection from surveillance (Interview, Senior Official, European Union, 2014), a policy supported by the growing "Pirate Party" movement (Interview, Senior Official, DG HOME, European Commission, 2014).

The protection of personal privacy is not simply a matter of engendering and promoting trust in digital systems, however. Privacy and data protection had been long-term concerns for the EU and acknowledged as fundamental rights to be protected alongside the freedom of speech and expression (Bangemann, 1994, p. 11; European Commission, 2007b, p. 1, 1997a, p. p.17, 1997c, p. 2; Interview, Massart, SDA, 2014; Interview, Senior Official, DG HOME, European Commission, 2014). By 2013, the communicative capacity of the

Internet and cyberspace had been demonstrated and acknowledged as a vital component against oppressive regimes. The EUCSS itself cited the Arab Spring as an example of the capacity of cyberspace to ensure that rights of expression and free speech are fulfilled and maintained (European Commission, 2013a, p. 2). Digital systems and infrastructures are therefore of critical importance not just for commercial and civilian life and interaction, but as a tool to exercise fundamental rights and pursue democratic governance. This importance is shown by the fact that during the Arab uprisings in 2011, the Egyptian government shut down the country's Internet access in an effort to curb the protests. The right to access and disseminate information became a major driver for the Arab Spring itself, particularly in Egypt (Olukotun and Micek, 2016).

The importance of protecting fundamental rights, as a driver for EU cyber security policy, therefore continued unaffected post-Lisbon. The only difference was that, after 2009, privacy was formally acknowledged as a fundamental right accorded to all EU citizens. Privacy was incorporated into the TEU and TFEU through recognition of the Charter of Fundamental Rights (European Union, 2009a, p. 397). The protection of such rights, in the context of cyber security, not only continued but was increased in importance after 2009. This did not, however, alter the EU's focus on this sector. Rather, it placed the respect for personal privacy and data protection alongside other basic human rights (Interview, de Vries, National Cyber Security Centre of the Netherlands, 2014).

Another avenue employed to engender trust in digital communications was the tackling of cyber-crime, one of the five core ideational elements of the EU's discourse. The Union's focus on illegal and harmful content addressed issues as diverse as the protection of children when online (European Commission, 2011c, 2010f, p. 3,4; Interview, Senior Official, DG HOME, European Commission, 2014; Interview, Senior Official, Europol, 2014) and digital piracy and copyright infringement (European Commission, 2010d, p. 8; European Council, 2011b, p. 2). Online piracy had increased in significance in this period, particularly due to the value of intellectual property in the information based economy (Meyer, 2012, p. 107). This shows that the ideational priority of tackling cyber-crime was also unaffected by the Treaty of Lisbon.

The only tangible change in tackling cyber-crime at this time came about irrespective of the Treaty. This was the elevation of Europol's high-tech crime unit into a dedicated European Cyber Crime Centre (EC3). While the activities of this Centre do not differ greatly from its predecessor, they were clarified. The EC3 now serves as the central hub

for criminal intelligence and information relating to online criminal activity. According to its website, there are three areas on which it has been tasked to focus:

- Cyber-crimes committed by organised groups, particularly those generating large criminal profits such as online fraud;
- Cyber-crimes which cause serious harm to the victim such as online child sexual exploitation;
- Cyber-crimes (including cyber-attacks) affecting critical infrastructure and information systems in the European Union (Europol, n.d.)

The approach of the EU to tackling cyber-crime post-Lisbon is therefore not dissimilar to that of the pre-2009 period. The EC3 still is not an executive law enforcement agency. It supports Member States in their own operations and investigations. It provides training and capacity-building as well as strategic analyses. At the time of the EC3's initiation, ultimate responsibility for identifying and prosecuting cyber-criminals continued to reside with the Member States' own law enforcement agencies, as was the case prior to 2009.

Not only does this demonstrate the continuity of the ideational element of cyber-crime post-Lisbon, the function of the EC3 maintains the EU's arms'-length approach to achieving cyber security. As an actor, the Union sought to facilitate information-sharing and co-operation through such hubs as the EC3 and ENISA (Interview, Purser, ENISA, 2014; Interview, Senior Official, EC3, 2014). Despite the Treaty of Lisbon extending the right of policy and legislative initiative as part of the removal of the Pillar structure, no extra authority or executive powers were afforded to Europol or the Commission.

The lack of extra powers and the continuation of an arms'-length approach are demonstrated by the fact that legislation in this sector was sparse post-Lisbon. After 2009, only five legislative instruments were passed. Three of these related to establishing large-scale initiatives such as the Horizon 2020 programme or extending ENISA's mandate (Council of The European Union, 2013c; European Parliament and Council of The European Union, 2013a). Formal legislation addressing criminal activity was limited to a Directive on child pornography in 2011 (European Parliament & Council of The European Union, 2011) and a Regulation promoting co-operation between Member States (European Parliament & Council of The European Union, 2012).

These measures not only imply the continuation of the EU's focus on cyber-crime post-Lisbon (despite a paucity of formal legislative instruments), they also demonstrated the continuation of the EU's operational methodology. The EU was not expanding or creating

executive powers of arrest in the field of cyber-crime, or seeking actively to secure resources or infrastructures from criminal activity. Instead, continuing trends established prior to 2009, the EU focused on establishing protocols and facilities for information-sharing and co-operation. A senior official from the UK's Foreign and Commonwealth Office stated that not only was this an area in which the EU could operate, but smaller, newer Member States *want* the EU to be involved in *this* capacity as this provides direction and coherence (Interview, Senior Official, UK Foreign and Commonwealth Office, 2014). As Smith and Jones state (Interview, Smith and Jones, eu-LISA, 2014), it makes sense, under the principles of subsidiarity, for the EU to be involved in developing coherence in this particular policy sector. This is due to the transnational, cross-border nature of cyber-crime activity. Cross-border activity cannot be tackled solely at the Member State level. Executive authority, in terms of specific technical solutions or powers of arrest, remains, however, with the Member States.

In order to achieve its policy goals – maximising economic potential, engendering trust, protecting rights and tackling cyber-crime – the EU continued another trend established before 2009. It sought to establish itself as an actor facilitating co-operation. Instead of physically providing security it would work to ensure that those actors with ultimate responsibility for the security and safety of infrastructures (the Member States and the private entities which owned and operated digital networks) shared information and best practice effectively and efficiently. Co-operation remained the primary *modus operandi* for achieving cyber security policy goals. The continued primacy of co-operation in cyber security can be demonstrated in a standard content analysis of Union *acquis*. After 2009, there are 229 references to co-operation in cyber issues. Of those 229 references, 34 were made in the EUCSS alone. The results of this analysis are shown in Table 9-1 below.

Table 9-1: Content Analysis of Occurrence of Ideational Elements 2007-2013

Element	Co-operation	Economics	Cyber-Crime	Rights	Trust
Number of Occurrences	229	120	91	63	45

While the focus on co-operation as a tool is a carry-over from the pre-Lisbon period, its presence *after* the entry into force of that Treaty highlights two important developments. The first is the larger role of the private sector in securing cyberspace. There is a notably

increased drive to involve private operators post-Lisbon, particularly in the area of system and infrastructure resilience. Measures to secure critical digital and physical infrastructures, such as the European Public-Private partnership for Resilience, specifically cited the enhanced role of the private sector in achieving cyber security (European Commission, 2011a, p. 6, 2010g, p. 10). Co-operation between public and private actors would form a substantial aspect of the EUCSS itself in 2013. Tunne Kelam MEP, as well as senior officials from the EC3, point to the increased attention paid to ensuring private sector involvement in the field of information exchange (Interview, Senior Official, EC3, 2014; Telephone Interview, Kelam MEP, 2014). The EC3 now operates as an information hub pooling and analysing intelligence from across the Member States. Outreach activities conducted by the Centre have resulted in so great an influx of intelligence and information from the private sector that there is now too much data to analyse. The EC3 has had to ask private operators to send *less* data (Interview, Senior Official, EC3, 2014).

This increased attention was due to an acknowledgement that, by 2009, elements of the digital infrastructure spanning the EU were owned and operated not by publically-owned utility companies but by the private sector (European Commission, 2009a, p. 5). In addition, much of the critical physical infrastructure underpinning EU functionality in general, such as energy, communications and transport, was similarly owned by private corporations. The content analysis of the total library of Union *acquis* showed an acceptance throughout the policy-making timescape of the need to involve the private sector. However, of the 12 items of *acquis* to specifically cite private sector involvement, five were published between 2007 and 2013. The importance of the private sector in *acquis* is corroborated in research interviews. Five of the interviews specifically attest to this important role.

The second important development in facilitating co-operation was the initiation in this period of a specific conduit for such co-operation and discussion which had the ear of the presidency of the Council of the European Union. In 2011 an unofficial body was established called the Friends of the Presidency on Cyber Issues (Interview, Permanent Representation of Germany to the EU, 2015). While the establishment of Friends of the Presidency (FoP) groups is neither a novel nor unusual development (there are FoP groups covering a range of policy sectors) what makes this an important development with regard to cyber security is the collection of actors involved in the group, and the high-level access it has to Council leadership.

The aim of FoP groups is to provide discussion venues on policy sectors for the formal institutions of the EU, operational agencies and national Member State representatives. These fora enable functional overlap between representatives to be avoided and discussions to be held without the restriction of competences (Interview, Senior Official, DG HOME, European Commission, 2014). In the FoP on cyber issues, functionaries from the EDA meet with counterparts in ENISA or the Commission to discuss each other's activities to avoid the kind of overlap the European Council identified as problematic in 2002 (European Council, 2002). A range of working groups made presentations at a meeting of the FoP in December 2012, including justice and immigration, telecommunications, industry and competition (Council of The European Union & Friends of the Presidency on Cyber Issues, 2012). This demonstrated the scope of discussions held in these groups, and their ability to facilitate better understanding of what each participant is doing. Given the range of actors involved in these meetings FoPs facilitate the development of coherence of action and policy (Interview, Senior Official, UK Foreign and Commonwealth Office, 2014). They can act as advisory panels for the Council Presidency. As such, FoP groups are potentially quite influential, despite being informal in the sense of not being officially instituted or mandated.

Quantifying the FoP on Cyber Issues' precise level of influence is challenging because it is an informal forum. Only one instance of its meeting agenda was identified for analysis in this thesis. Furthermore, EC3 officials acknowledged that the effectiveness of FoP groups such as that for cyber security depends on the enthusiasm of the sitting Presidency for the topic under discussion (Interview, Senior Official, EC3, 2014). Due to the system of rotating leadership, an FoP group for a policy sector not considered a priority by the current Council Presidency will be less influential than that of a sector considered vital. The important point here is that the very fact such a body exists is testament to the importance placed on cyber security by the Union, and testament to the need for co-operation as a methodological tool and policy aim in this sector.

Cyber security policy post-Lisbon was not radically different from its previous iterations. There were specific innovations in this phase, such as the elevation of Europol's high-tech crime centre to a formal pan-European Cyber-Crime Centre, the 2011 establishment of a Friends of the Presidency Group, and the confirmation of privacy and data protection as fundamental rights afforded to each citizen. These innovations, however, did not detract from the EU's underlying socio-economic discourse. There was no focus on military or defence issues. Those incidents which could potentially have been treated as national

security threats, for example the Snowden revelations, were perceived as threats to citizen privacy from over-zealous state surveillance. In other words, they were still interpreted as socio-economic in nature.

Furthermore, the elements used to frame this discourse also had not changed. There remained a focus on maximising economic opportunities afforded by cyberspace, but also ensuring that citizens and corporations trust digital and online systems. Protecting fundamental rights and tackling cyber-crime would go some way to ensuring this trust. The EU's method of choice to achieve these aims was to continue to be a facilitative actor, bringing entities together to ensure that information, intelligence, experience and best practice continued to be shared.

It is therefore clear that the Treaty of Lisbon did not radically alter the EU's cyber security policy discourse. The five core ideational elements underpinning it remained static, while the EU's structure was radically altered. This raises the questions of *why* and *how* this lack of impact came about. The answer to these questions is the static, unchanging nature of Union competences.

9.4.2. The Nature and Influence of Competence Post-Lisbon

Far from being changed or amended in the face of major exogenous crises, the EU's socio-economic cyber security discourse was further entrenched. This can be seen in the interpretation the EU placed on events in 2007 and 2008 in order to be able to develop responses within its competences. An important example was the EU's interpretation of the cyber-attacks on Estonia in 2007. The Estonian government classified this incident as a risk to national security. The EU, however, had no competence to engage with a national security incident. It therefore approached the issue from a socio-economic perspective. This was a perspective born of a cyber security discourse developed over the years prior to 2007. The attacks on Estonia were interpreted as existential threats to the functioning of the Single Market and the EU's economic viability as a whole. This placed the incident *within* the EU's socio-economic competences. From an historical institutionalist perspective, this is unexpected. Policy paths tend to shift and change due to the occurrence of major events and crises (Peters, 2005, p. 83). In EU cyber security, however, the path dependency of the EU's competence-defined narrative was so strong that instead of changing, the path was consolidated and employed to enable the EU to respond to an exogenous issue out-with its normal remit.

Despite being a major event *endogenous* to the EU, the Treaty of Lisbon also advanced policy-making in this sector but did not effect any changes to the underlying policy discourse. The Treaty created an architecture amenable and conducive to the development of the EUCSS by removing the Pillar structure instituted by the Treaty of Maastricht. It is fair to say that without this removal the EUCSS would never have been published in its 2013 form. However, despite these major architectural changes which became effective in 2009, the EU's underlying discourse in cyber security as a policy sector remained unaltered. There continued a focus on socio-economic aspects of security such as ensuring the economic and functional viability of the Single Market, protecting citizen rights and tackling cyber-crime. The solution of choice – facilitating co-operation between actors – continued from its pre-2009 foundations. The unchanging nature of these core ideational elements meant that the EU's underlying discourse was also unchanged.

The EU's cyber security discourse therefore remained resilient in the face of these major events. There were no extra powers afforded to the EU as an international body in the face of apparent state-sponsored cyber-attacks in Estonia, or as a result of the new single, legal personality created by the Treaty of Lisbon. The EU's policy response to cyber security remained one predicated upon maximising economic opportunities, eschewing defence or military issues, and interpreting events as threats to the Single Market.

Not only did that discourse weather the major events of 2007, 2008 and 2009, but it coalesced to form the foundations for the EU's first formal, holistic cyber security strategy, the EUCSS published in 2013. Analyses of the Context chapter of that document demonstrate that the five core ideational elements which construct the EU's socio-economic discourse underpin the purpose, background and overall content of the EU's holistic response to cyber security (See Chapter 5 Section 2).

The static nature of this discourse has particular ramifications for the theories applied to this research. As examined in Chapter 4, the concept of "punctuated equilibrium" refers to moments of crisis which effect change in an otherwise stable and static policy path (Krasner, 1984, p. 240). Large-scale departures from policy paths occur in response to important events or crises (Baumgartner et al., 2014, p. 59). The major events in the EU's cyber security policy-making process certainly advanced that policy, but did not punctuate its equilibrium in the manner anticipated by Krasner and Baumgartner. Instead, these punctuation points served to further entrench the EU's underlying discourse to the extent that it informed the Union's interpretation of those events. Although the EU's operational

approach evolved and demonstrated elements of change there was no departure from the fundamental discourse the EU constructed around cyber security. The policy discourse continued even in the aftermath of the Treaty of Lisbon, an event which punctuated the equilibrium of the Union's entire policy-making and existential architecture.

There are two reasons for this seemingly paradoxical effect. The first is the long-standing institutional path dependency of the EU's discourse in this policy-sector, a discourse predicated upon five core ideational elements. The examination of that discourse in Chapter 5 demonstrated the conceptual continuity running throughout the 28 year timescape, inferring an ideational path dependency inherent in the EU's developing response to cyber security challenges.

The second reason that the Treaty of Lisbon did not, and could not, affect the EU's discourse in this sector is one of greater importance to this thesis. The Treaty did not affect or amend the Union's discourse in this sector because it did not expand, enhance or otherwise change the EU's fundamental competences. The Lisbon Treaty clarified, codified and explained those competences, and the policy sectors in which they apply, but did not grant the EU any extra capabilities in those sectors. This is particularly the case in foreign and security policy. The Common Foreign and Security Policy (CFSP), a jealously-guarded area of exclusive Member State competence pertaining to national security, was left largely unchanged after the Treaty of Lisbon (Craig, 2010, p. 182). Its separate nature was codified as an area of "special" competence, sitting out-with the normal triad of exclusive, shared or supporting competences. There was no scope for any expansion of authority or capability into military, defence, or national security considerations. This meant that a socio-economic discourse towards cyber security was the EU's only option. The EU's competences were an institutional constant throughout the entire timescape of 1985 to 2013 and their unchanging nature led to the *entrenchment* of the EU's discourse in this policy sector. This entrenchment and path dependency was so strong that exogenous crises such as the cyber-attacks on Estonia in 2007 and the financial crash of 2008 failed to punctuate those paths.

The effect of Union competences on EU cyber security is to serve as an anchor for the discourse in that field and the five underlying ideational elements. The path dependency affecting these elements was strengthened and reinforced between 2007 and 2013 despite being exposed to severe internal and external stresses because the primary institutional dynamic – competences – were not altered.

9.5. Conclusion

Between 2007 and 2013 the EU's cyber security policy-making process was exposed to severe institutional stresses. Events which began outside the Union – the 2007 Estonian cyber-attacks and the 2008 global financial crisis examined in Chapter 8 – tested the EU's ability to respond to cyber security incidents. The nature of its response demonstrated two important aspects of Union policy. First, its responses were based on *interpretations* of the incidents as threats to the viability of the Single Market. Even an event such as alleged Russian cyber aggression against Estonia, described as an attack on sovereignty by the victim nation, was classified as a threat to the ongoing functionality of the Single Market. This was due to the Single Market's reliance on resilient ICT infrastructures. The economic importance of ICT was further demonstrated by the focus placed on that sector as a commercial domain following the start of the 2008 financial crisis. In a move reminiscent of the 1980s, specific attention was paid to the ICT sector to stimulate growth and employment.

The second aspect highlighted by these responses is the EU's restricted security competences. The reason for the EU adopting this interpretive, socio-economic approach was because it was confined to addressing socio-economic aspects of foreign and security policy by the 1987 Single European Act and the 1992 Maastricht Treaty. In 2007 and 2008 the EU had a limited range of policy options at its disposal. Put another way, the nature of the EU's competences in security matters required it to interpret major international incidents such as "Estonia 2007" and the 2008 crisis as socio-economic threats. The path dependencies initiated in the early stages of policy development in this sector – the importance of ICT to the Single Market and a restriction of competences to socio-economic matters – necessitated a particular response to important exogenous crises. This was the result of the development of an idiosyncratic cyber security discourse, itself the result of these policy paths.

However, the nature of Union policy in this sector after the entry into force of the Treaty of Lisbon in 2009 further demonstrated the strength of these policy paths. The Union's discourse continued despite the fundamental changes ushered in by that Treaty. Even with the removal of the Pillar system of policy development instituted by the Maastricht Treaty and the direct, Treaty-based clarification of competences, the EU's cyber security policy continued to be socio-economic in nature.

The chapter also made two observations. The first is a direct answer to the research question: Union competences led the EU to develop a particular, socio-economic discourse and approach to cyber security challenges, and also led to the continuation of that approach.

The second important observation is there are ramifications for historical institutionalism due to the strength of Union path dependencies. As examined in Chapter 4, the notion of path dependency is predicated upon the idea that policy choices lead to periods of consolidation and stability until a shock – a punctuation point – occurs which then causes policy change generating a new period of consolidation. Punctuated equilibrium goes some way to explaining policy change. The paths initiated by the EU in cyber security, however, were so entrenched that they withstood exposure to three very different but no less significant punctuation points, and continued unaffected, even becoming *further* entrenched. This demonstrates that path dependency and punctuation points can go some way to explaining policy continuity, as well as policy change. The final chapter of this thesis will explore these observations in order to demonstrate the influence of this research on both EU policy-making literature and historical institutionalist scholarship.

Chapter 10 | Conclusions

10.1. Introduction and summary of main findings

This thesis opened with a comment on the 2016 *Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*. This Directive established a set of rules for addressing cyber security in the EU and built on the influential 2013 *Cyber Security Strategy of the European Union* (EUCSS). Not only did this Strategy identify the importance of cyber security for the Union in a number of areas, including in the context of its Digital Agenda, it set out for the first time a holistic Union approach to security issues in cyberspace.

That approach had developed over the previous 28 years and, while other actors added national security, military or defence considerations to their responses to cyber security challenges, the EU adopted and maintained a socio-economic policy discourse. This discourse and its continuity led to the research question this thesis sought to answer: *have institutions and institutional arrangements led the EU to develop and continue with a socio-economic approach to cyber security?* In order to answer this primary question, three supplementary questions also required to be addressed: which institutions had the greatest influence on EU cyber security policy; did any non-institutional elements also have an influence; and was there any interplay between these institutional and non-institutional elements?

There were three main findings which resulted from the research carried out to answer these questions. The first two of these findings constitute an **empirical contribution** to the study of the EU and its policy-making processes. They reflect the specific goal of the thesis and emerged as a result of what it sought to explore: the influence of institutional dynamics on a particular policy area. The first finding answers the first supplementary question for this thesis: which institution had the greatest influence on EU cyber security policy development and continuity? The analysis conducted identified that the EU's competences were the institutional drivers of greatest influence in this policy sector. The system of exclusive, shared, supporting and special competences established a policy framework in which the EU was restricted to non-military, socio-economic policy choices. The result of this restriction was that only socio-economic considerations in cyber security could be developed and implemented. This provides a direct, but over-simplified answer to the primary research question, one which takes no account of timing.

The second finding is the confirmation of the existence of a specific cyber security discourse based around five core ideational elements: economic maximisation, the protection of fundamental rights, engendering trust in digital systems, tackling cyber-crime and facilitating co-operation. These five elements inform *all* policy in this field. They are present at the initiation of Union interest in ICT in 1985 and continue into the publication of the EUCSS in 2013. This discourse therefore represents ideational continuity throughout the 28-year timescape. Crucially, the influence of these ideas on cyber security policy began *before* the Union's socio-economic competences began to be formalised. The confirmation of a discourse built around a set of ideational elements, and their continuity throughout the policy development timescape, answers this thesis's second supplementary question: were there other forces at work – particularly ideational or catalytic elements – which inform policy choices?

There is therefore a deeper, more nuanced answer to the research question than simply "the competences led to the EU's policy". This deeper answer stems from the confirmation of *both* institutional and non-institutional influences on EU cyber security policy development and continuity. This deeper answer acknowledges the importance of timing and sequencing and addresses the third supplementary question for this thesis: did any *interplay* between institutional and non-institutional policy drivers also have an influence on the reasons why the EU developed and continued its socio-economic cyber security discourse? The EU's socio-economic interest in ICT began with the initiation of the Single Market programme in 1985. However, once Union competences began to be formalised between the 1987 Single European Act (SEA) and the 1992 Maastricht Treaty, other policy options or approaches were no longer available. The established socio-economic approach to ICT became the only manner in which the EU could tackle developing cyber security challenges, regardless of how those challenges or the sector developed. As a result of this particular mode of interaction, that discourse continued unchanged between 1985 and 2013 because the institutional framework of competences did not enable it to change.

This ideational and institutional interaction and the resulting institutional stickiness of the EU's discourse led to a third finding. This is a **theoretical contribution** to historical institutionalist scholarship. As described above certain policy choices, namely the codification of competences, meant that other policy options and approaches to cyber security were no longer available to the EU. Path dependencies had been established and were locked in place. Thus far, EU cyber security policy conforms to certain theoretical models of HI, namely that choices made early in a social process continue to have an effect

later in the timescape. However, during the data analysis for this thesis cyber security policy was found to be highly resilient to major exogenous and endogenous shocks. These shocks would normally have generated policy change, a process known as *punctuated equilibrium*. In a break from standard models of punctuated equilibrium, instead of changing policy, the response of the EU to these shocks and crises was to further *entrench* established policy paths.

This unexpected finding has important implications for HI as a theoretical approach to the study of the EU: cyber security as a policy sector did not follow the standard models of punctuated equilibrium. Instead of changing to new policy paths, the EU's approach continued and was strengthened as a result of the occurrence of the major events of 2007-2009. Punctuated equilibrium, in this case, goes some way to explaining policy continuity, rather than policy change. It therefore provides a more flexible model for examining and explaining social phenomena than may at first be apparent.

This final chapter has six sections. Following this introduction, the three main findings of this thesis are set out in turn. Sections 2 and 3 set out the empirical findings of the research and expand on the partial answer to the research question – that Union competences influenced policy development – to set out *how* this influence occurred and, most importantly, *why*. The fourth section of the chapter reflects on the theoretical findings of the thesis and examines its resulting contribution to historical institutionalism.

The fifth section of the chapter examines the implications of these research findings. In particular, the section looks at the practical contribution the thesis can make for policy practitioners and scholars working in the historical institutionalist tradition and proposes avenues for further research.

The sixth and final section concludes by setting out the empirical, methodological and theoretical contributions this thesis makes to current academic scholarship. The thesis examined EU cyber security policy, an under-researched aspect of the Union's extensive remit, and sought to explain *why* the EU approaches cyber security in the manner that it does. This was done in order to expand current literature which focusses on *how* the EU approaches cyber security challenges. The thesis also makes a methodological contribution to the study of social and political phenomena: a conceptual content analysis technique was developed specifically for this thesis. This technique can be applied to other areas of policy development in the EU and beyond. To facilitate this methodology, a new model of "actorness" was developed that blends elements of the work of Scharpf, Bretherton and

Vogler (Scharpf, 1997; Bretherton and Vogler, 2006). In terms of theoretical contributions, the thesis applied historical institutionalism (HI) to cyber security and found that a specific mechanism of HI, punctuated equilibrium, can help to explain policy continuity, as well as policy change.

10.2. Finding 1: Socio-economic competence as the institutional driver of greatest influence on EU cyber security

In order to answer the research question it was first necessary to determine which if any institutions had any influence on EU cyber security policy. As set out in Chapter 3 this thesis used Hall's (1992, p. 96) definition of institutions as formal rules, standard operating procedures and customary practices which affect actor behaviour and effect policy choice. Following this definition, the Treaty-defined competences of the EU were identified as the institution of greatest influence in this particular policy sector. Divided into four types, the competences define in which areas of policy the EU can become involved, and to what extent. As examined in Chapter 4 Section 2.1, in areas of exclusive competence[58] the EU alone is able to legislate and adopt binding acts. In areas of shared competence[59], the EU divides this ability with the Member States while in areas of supporting competence[60] the EU can only advise the Member States. The CFSP comprises an area of "special" competence, where EU action is severely limited.

Union competences therefore provide a set of rules and standard operating procedures (institutions) which led the EU to develop a particular interpretation or construction of cyber security risks and threats. So strong was the influence of Union competences on cyber security policy that they created an institutional structure in which the only policy solution available was a socio-economic discourse. The 1987 Single European Act and 1992 Maastricht Treaty confined the EU to political and social aspects of security and restricted its capacity to address foreign and security matters. This situation contributed to the organic evolution of a particular discourse of cyber security policy (examined in Finding 2 below).

Not only did Union competences influence the development of a socio-economic discourse, they perpetuated it. Between 1985 and 2013 the discourse would remain unchanged and be applied in the development of successive cyber security strategies and

[58] Such as the customs union, competition policy and fisheries
[59] Such as the internal market, transport policy and technological research
[60] Including culture, tourism and education.

proposals in 1996, 2001 and 2006. This eventually culminated in the discourse's application in the development of the EUCSS in the early 2010s. The restricted competence in defence matters persisted throughout the timescape. As a result the discourse could not evolve or expand to include "cyber defence" or any national security-focussed elements. The static nature of Union competence meant that the socio-economic discourse was the only set of policy options which could be applied in the event of cyber security incidents or crises. Such incidents and crises subsequently needed to be interpreted in a fashion that enabled the EU's discourse to be applied. As examined in Chapter 8, this was the case with the DDoS attacks on Estonia in 2007. Although the victim state described the incident as a national security threat and a defence issue, the EU interpreted it as a risk to the economic and functional viability of the Single Market.

10.3. Finding 2: Clarifying the EU's Cyber Security Discourse

The second empirical finding is that the EU's cyber security discourse, developed between 1985 and 2013, was constructed around five specific ideational elements. These are: a focus on maximising the economic potential of cyberspace; engendering trust in new technologies and ways of doing business; protecting fundamental rights such as privacy; tackling cyber-crime; and achieving these aims through facilitating co-operation across Member States at both national and corporate levels.

These five ideas are policy norms which lie at the heart of EU cyber security policy throughout the entirety of the policy development timescape. Using a conceptual content analysis technique developed specifically for this research it was possible to identify not only the ideational elements themselves, but also their pervasive, continuous presence in both *acquis* documentary and interview data sources.

The reason these five ideational elements are important for this discourse is that they are not just present or identifiable in certain examples of the Union's *acquis communautaire*, but form core components in ***all*** relevant *acquis*. They are particularly prevalent in the first three attempts to develop a cyber security strategy prior to 2013: the 1996 *Commission Communication on illegal and harmful content*; the 2001 *Proposal for a Network and Information Security Strategy*; and the 2006 *Strategy for a Secure Information Society*.

A crucial aspect of this composite discourse is that it is one which eschews martial language and focuses on socio-economic aspects of security. The EU is not a military organisation and so a lack of military language is not surprising. However, this statement

oversimplifies the reasons for the EU not using such language in cyber security policy. The deeper reason behind the lack of martial language in this policy area is because the five core elements underpinning that policy are themselves socio-economic in nature. There were few references to national security or military issues beyond mentions of terrorism in 1996 and 2001 or the need to develop partnerships with military allies such as NATO in 2013. Throughout the entire 1985-2013 timescape, and the *acquis* developed within it, there was no use of language such as "cyber war", a term coined by Arquilla and Ronfeldt in 1993 (Arquilla and Ronfeldt, 1993). Instead, cyber security challenges, such as those faced in the years between 2007 and 2009[61], were *interpreted* as socio-economic threats. This interpretation occurred because of the Union's socio-economic discourse, one in which there was no scope or capacity for martial language.

10.3.1. Empirical Implications: The influence of competences and ideas on EU cyber security policy development

The research question for this thesis is: *have institutions and institutional arrangements led the EU to develop and continue with a socio-economic approach to cyber security?* This question arose due to the EU developing and maintaining a socio-economic cyber security discourse while other state actors have added national security, military and defence considerations in response to the same challenges. An initial observational answer to this question is: the EU's Treaty-based competences have led the EU to the development and continuation of a socio-economic discourse. As set out in Finding 1 above, the competences define in which policy areas, and to what degree, the EU can operate. As a set of rules and standard operating procedures, the competences bestow great freedom of engagement in socio-economic policy areas, at the expense of military or national security areas. Therefore Union competences confined the EU to socio-economic aspects of cyber security with very few details on military or defence matters.

This answer, however, belies the complexity of the relationship between competences, ideas and the EU's cyber security discourse. It also takes no account of timing. In gathering data sources and tracing the progression of the EU's policy in this sector the empirical chapters of this thesis demonstrated that the EU's socio-economic interest in ICT – what would evolve into cyber security policy – began with the initiation of the Single Market in 1985. This was two years *before* the entry into force of the Single European Act (SEA) when security competences began to coalesce. Historically, this concentration on economic, social and industrial policy was a throwback to the failure of the European

[61] See Chapters 8 and 9.

Defence Community (EDC) in 1954. According to Dinan (2010, p. 21) the EDC would have enabled collective defence and security action in a similar vein to its counterparts, the European Coal and Steel Community (ECSC) and the European Atomic Energy Community (EAEC). Because the EDC had foundered after being rejected by the French Parliament, there was no definitive clarification of European capacities in defence and security[62]. These sectors were omitted from the precursors to the modern EU. As a result of this omission, the EU's security remit remained unclear until the mid-1980s. That clarification came in the 1987 SEA and 1992 Maastricht Treaty but occurred separately to, and crucially *after*, the initiation of the EU's discourse in what would become cyber security.

Two processes were occurring in parallel to one another, both as a result of the EU developing a policy of economic integration post-1985. First, the EU was embarking on a large-scale economic restructuring because it was, at its heart, an economic entity. This led to the EU developing its interest in ICT as a sector for economic growth and increased employment. Cyber security policy would evolve from this discourse. Second, the Union was clarifying and codifying its restricted security capacities and competences, also the result of the EU developing this economic policy narrative.

By the time the Commission published its Communication on illegal and harmful online content in 1996 these two parallel processes of economic development and codification of competences had intersected. The codification in the 1992 Maastricht Treaty of the restriction of policy-making capacities to the economic and social aspects of cyberspace had important effects on EU cyber security policy. It meant that *subsequent* policy could only address these aspects. This restricted the EU's discourse in that sector. By 1996 the five core ideational elements identified in Finding 2 had become core features of the EU's cyber security policy[63]. With the entry into force of the Maastricht Treaty that discourse was locked in place. Union competences established and formalised between 1987 and 1992, two years *after* the initiation of the internal market and the commencement of EU interest in ICT, put the EU on a policy path from which it would not deviate. This lack of deviation, or strength of policy path dependency, would be demonstrated 20 years later when the EU faced the Estonian attacks of 2007, the financial crisis of 2008 and the entry into force of the Treaty of Lisbon in 2009. Despite these three significant institutional stresses, including a major restructuring of the Union and removal of policy pillars, the

[62] A possible exception to that was the Western European Union (WEU). However, as the European arm of NATO this was a separate entity to the developing EU.
[63] See Chapter 6.

EU's cyber security discourse did not alter. This was due to the strength of the institutional lock of unchanging, static competences. Because competences did not change, neither did the cyber security discourse.

There are two consequences of an interaction of static competences and a specific policy discourse. First, that interaction meant that cyber incidents had to be *interpreted* in a socio-economic manner by EU policy-makers in order for the Union to be able to respond. This interpretive act was most evident in one particular event, the EU's response to the DDoS attacks on Estonia in 2007. At the time the EU interpreted that event not as a military threat necessitating a defence-policy response, but as an economic threat to the ongoing functionality and viability of the internal market. Doing this enabled the EU to co-ordinate a response. This act demonstrates the existence of a mechanism which enables EU policy-makers to engage with topics and issues in which the Union has limited competences, or even with matters outside its purview. By engaging with a policy area interpreted as socio-economic, the EU is increasing the legitimacy of that involvement.

Secondly, in historical institutionalist terms, the unchanging nature of its competences meant that the EU could not divert from paths established in the earliest stages of the policy process. Path dependency had been created based around five core ideational elements. This further demonstrates that the institution and institutional arrangement which had the greatest influence on the EU's cyber security policy was the Union's competences. Their unchanging nature led to the *entrenchment* of a particular narrative approach to cyber security which underpinned all the EU's policy in this sector.

The answer to the research question for this thesis is therefore ***not*** simply "the competences of the Union" (despite this view being held by a number of interview participants). The precise relationship of the EU's cyber security discourse with those competences is more complex than that statement suggests. The Union's competences and its cyber security discourse were born of the same general socio-economic direction begun in the 1980s. That direction led to a clarification of policy remits and capacities for the Union which would evolve into a set of rules, standard operating procedures and patterns of behaviour. These would be of greater influence on the future development of cyber security policy than the cyber security discourse itself. Competences would lock the EU's discourse in place, tying its expansion, or lack thereof, to their own development. Where the competences went, so too would go the EU's cyber security discourse.

10.4. Finding 3: The resilience of EU cyber security policy to institutional stresses

This institutional lock leads to a third finding, one which makes an important theoretical contribution to both EU scholarship and historical institutionalism (HI). It relates to punctuated equilibrium, an important aspect of HI approaches to the study of political processes. Under the mechanisms of path dependency, choices made at the initiation of a policy or process continue to affect that policy in later years. In the case of EU cyber security this thesis has shown that that process began with the initiation of the internal market in 1985 and the promotion of ICT as a commercial domain throughout the 1990s, and was heavily influenced by the development and codification of Union competences.

Once these choices were made, the policy sector entered a period of consolidation, or equilibrium, between 2001 and 2006. During this time EU policies of tackling cyber-crime and fostering co-operation were entrenched and operationalised through the establishment of dedicated agencies such as ENISA and the high-tech crime centre at Europol.

At this point, however, EU cyber security policy ceases to conform to the mechanisms of punctuated equilibrium. Under those mechanisms, once path dependency in a policy area has been established, that policy becomes entrenched or "sticky" (Pierson and Skocpol, 2002, p. 7). It is subject to institutional inertia and it is difficult to alter or amend policy choices without a major impact – a punctuation – occurring which can cause changes in policy choice and direction. Krasner (1984, p. 240) argued that when policy paths are punctuated by major events, new paths are created. This is how policy choices are changed.

In EU cyber security policy, such punctuation points occurred when the cyber-attacks on Estonia took place in 2007, the financial crisis began in 2008 and the Treaty of Lisbon entered into force in 2009. Within the context of punctuated equilibrium, these events should have led to changes in the EU's cyber security policy paths. What actually occurred was that these paths continued and were further consolidated. The reason for this was that Union competences and the five ideational elements of cyber security did not change between 1985 and 2013. The only major opportunity to amend competences – the Treaty of Lisbon of 2009 – did not alter the policy areas and capacities of the EU. Instead the Treaty clarified and codified its existing capacities, making it clear in which policy sectors, and to what extent, the EU could act. The EU's fundamental socio-economic discourse in this sector was unchanged after 2009 and actually became further entrenched.

This entrenchment following the occurrence of three major events is a significant divergence from punctuated equilibrium. Instead of policy paths changing to new states of equilibrium following the occurrence of major critical junctures, in the case of cyber security the opposite occurred: previous policy choices continued and were written into new, definitive strategies such as the EUCSS.

10.4.1. Implications for Historical Institutionalism

The third finding of this thesis raises important implications for HI as an explanatory theory for EU policy making. EU cyber security policy conforms to core elements of HI, such as path dependence and institutional "stickiness" (Alexander, 2001, p. 251; Pierson and Skocpol, 2002, p. 7). There is, however, a significant departure from certain aspects of HI, notably punctuated equilibrium. For HI scholars, this means that EU cyber security policy is an exception to standard models of punctuated equilibrium. This raises opportunities for studying the strength of institutional dynamics in the face of punctuation points which would normally break continuity and cause change.

The departure of EU cyber security from aspects of punctuated equilibrium is shown in the Union's response to the cyber-attacks on Estonia in 2007, the financial crisis of 2008 and the entry into force of the Treaty of Lisbon in 2009. These events had important effects on cyber security in general and on the structure of the EU itself. It was not unreasonable to expect that they would alter the direction of EU cyber security policy. What actually happened was that the EU's socio-economic cyber security discourse continued unchanged on paths established *prior* to 2007. Between 2007 and 2013 such policy and legislation as was developed further solidified the application of the discourse's five core ideational elements. As shown in Chapter 5 Section 2, this entrenchment can be seen in the Context section of the EUCSS itself. That section specifically utilises the five ideational elements of the EU's cyber security discourse as the underlying framework on which the EUCSS was developed. The implication is that the ideational foundations and concomitant institutional inertia of EU cyber security policy were so strong that they withstood the pressures and stresses experienced between 2007 and 2009. Cyber security policy can therefore be held up as an example of a process with institutional forces of exceptional strength.

While punctuated equilibrium is a tool for explaining policy change, this thesis has demonstrated that it can be used to explain policy continuity. The events which occurred between 2007 and 2013 clearly punctuated the equilibrium of the EU's approach to cyber

security. However, the EU's reaction was to strengthen its policy discourse. It did not re-evaluate its fundamental socio-economic approach, but instead used it to interpret external aggression as an economic threat in order to be able to produce a response. Similarly, the codification of the EU's competences in the Treaty of Lisbon could have been seen as a further restriction on its capacity to act in cyber security. Instead it was used as an opportunity to develop a truly holistic cyber security strategy *within* the framework of those restricted competences, something which could not have been done without the removal of the Maastricht Pillar system. That new holistic strategy was predicated upon a *continuation* of the underlying socio-economic discourse. EU cyber security policy was therefore resistant to the punctuation points and critical junctures of the 2007-2013 period.

This does not mean that either the model or mechanisms of punctuated equilibrium are flawed or deficient, or that a radical re-evaluation is required. The opposite is the case. By providing a tool to explain policy continuity, punctuated equilibrium is shown to be a more flexible and applicable tool which can be applied to a wider range of social and political phenomena. This means that the findings of this thesis make a contribution to the development and progression of HI as an analytical approach by expanding the explanatory potential of HI mechanisms. It also opens up potential avenues for further research. Future examinations of other areas of EU policy can identify whether cyber security is an aberration in standard HI processes such as punctuated equilibrium, or whether there are other policy sectors where critical junctures are shown to reinforce continuity rather than cause change. If this is the case then EU cyber security policy can be held up as an exemplar of an under-explored aspect of HI analysis.

10.5. Implications of this research for policy practitioners and avenues for further research

This research is important because it looks at *why* a particular policy solution was chosen. Policy and strategy in the EU are structured by and around Union competences. This thesis does not deny this fact. What the research has done is unpack the relationship between competences as an institutional driver and a finished policy product, in this case the EU's 2013 *Cyber Security Strategy*. In doing so, the research has shown that competences act in concert with key ideas, laid down at the initiation of a policy process. This thesis therefore provides greater insight by delving deeper into the policy-making process and makes a generalizable contribution to potential future analyses of international relations and political studies, including those beyond the European Union.

This is important for two reasons. First, such a study has not been carried out in EU cyber security research. This thesis has therefore provided a deeper, more nuanced understanding of EU cyber security policy-making. Second, the inter-relation of competences with important ideational drivers can now be examined in other policy areas. There are scores of sectors and areas in which the EU is involved. These range from agriculture to sports and tourism. It is not possible to say definitively whether or not the features identified in cyber security – it being a long term process with core ideational elements and an idiosyncratic discourse – are traits unique to that sector. The methodology for this thesis can be employed to extract the ideational elements and policy-making timescapes for other areas of EU policy. Not only would this exercise provide insight into those other policy sectors, but it would determine whether EU cyber security policy is unique in its development.

This thesis can therefore facilitate the understanding of not just *how* a policy or solution functions and came to be chosen, but *why*. A methodology has been developed involving a conceptual content analysis of relevant policy documents published over a longer period of time than may at first be evident. This longitudinal analysis can be employed to identify institutional and ideational drivers which have influenced policy *in conjunction with* Union competences. This is an area of potentially fruitful future research which will deepen the understanding of EU policy-making mechanisms.

The findings of this thesis are also important for policy-making practitioners in the EU itself. As set out in Chapter 3, bureaucrats are not in position for the entire duration of a policy timescape. They are therefore not always able to break the path dependency of policy solutions which have been developed prior to their engagement. This thesis has exposed the underlying institutional and ideational dynamics in cyber security policy. There are, however, both positive and negative implications of an increased clarity and awareness of underlying ideas and discourses in policy. As shown in this thesis, the existence of an underlying discourse allows for continuity of policy solutions, which in turn promotes stability of action. Throughout the 28-year timescape the EU has consistently advocated for more co-operation in cyber security, and has set itself up as a facilitative actor to promote that co-operation. This role has not changed, representing a stable anchor in a rapidly changing and evolving policy sector. This is a positive feature of the identification of underlying policy discourses.

A second positive point stemming from the identification of institutional dynamics is the recognition that these dynamics have been of influence in this sector for decades and can be forgotten over time due to the turn-over in employment of policy-making functionaries. This is not to say that this cycle cannot be broken. By being aware of underlying policy paths as a result of research such as this thesis, and the manner in which those paths interact, policy-makers have the opportunity to develop more creative solutions to cyber security problems. This fact is not restricted to cyber security policy. A greater awareness of the potential existence of underlying institutional currents in *all* areas of Union policy can be of benefit to practitioners in those sectors.

There are, however, less positive aspects of this institutional and ideational endurance. It should be pointed out that that same stability of action resulting from a continuous ideational background can reflect a certain inflexibility in developing policy solutions. Throughout the thesis, the argument has been made that the EU's competences have remained static and focussed on socio-economic matters. This has not enabled the EU to develop as effective a defence policy in cyber security as would be the case were the institutional frameworks of the competences more flexible. The EU's greatest strength – its institutional framework in which it can focus its efforts on socio-economic solutions of benefit to commerce and EU citizens – can also be considered its greatest weakness. Union competences have locked potential choices and solutions out of the development process. Once again, by being aware of the positive and negative aspects of institutional strength and by being more self-aware of the underlying dynamics of policy development, more creative solutions *within* those dynamics can be developed.

10.6. Contribution of the thesis and concluding comments

The aim of the research presented in this thesis is to contribute to an improved understanding of the EU's policy-making processes in the field of cyber security. The study of this sector provides insight into the EU's long-term policy-making process. Specifically, the thesis sought to explain *why* the EU adopted a purely socio-economic approach to cyber security when other actors included defence-oriented options. This is an original endeavour and as such the thesis makes a number of contributions to scholarship.

EU policy sectors such as agriculture, the environment, competition regulation or foreign and security policy have been the subject of extensive research, including analyses from specific theoretical traditions. Cyber security by contrast has received comparatively little

academic attention. Despite the speed of technological change in digital and online spheres, it was only recently that certain major events placed the security challenges of cyberspace at the top of political agendas and discussions. This thesis contributes to current scholarship by focussing on an under-researched policy area.

Cyber security was also not considered a stand-alone topic in academic studies of the EU and security. Such literature as currently exists on cyber security policy in the EU has approached the topic from a relatively narrow perspective. Contributions such as those of Christou (2016), Olesen (2016) and Sliwinski (2014) present interesting and valuable explanations for *what* the EU does in cyber security policy. Crucially, however, that literature has never offered a convincing reason for *why* the EU has adopted its particular policy approach. By undertaking an historical institutionalist analysis of this policy area this thesis has shown that it is possible to trace the development of cyber security within EU policy structures, and in doing so explain both *why* the EU adopted its socio-economic approach and why it continued.

The thesis also made a number of methodological contributions to scholarship. An analytical technique – a conceptual content analysis based on the work of Hycner and Berg (Berg, 2004; Hycner, 1985) – was developed for this research. This was done in order to study a policy area which suffered from a lack of agreed terminology and definitions, as well as examine literature and interview sources in equal measure. By searching for and counting the occurrence of synonymous concepts rather than individual words, a more nuanced, conceptual content analysis was developed that can be of benefit to researchers in a range of social science fields. This methodological tool can be applied to other areas of scholarship which are similarly handicapped by inconsistent terms.

The thesis also developed a method for testing the "actorness" of entities, the Scharpf-Bretherton-Vogler model[64]. This was developed by combining Scharpf's conceptualisation of "composite actors" with Bretherton and Vogler's three-part model of "actorness": opportunity, presence and capability. The model developed can be used to clarify the "actorness" of an entity not normally considered an actor in international relations, such as the formal institutions of the EU.

The thesis also made a theoretical contribution to scholarship relating to the use of punctuated equilibrium to explain policy continuity rather than change. By looking at the *response* of the EU to critical junctures and punctuation points, rather than the *impact* of

[64] See Chapter 4 Section 3.

those punctuations, it has been possible to clarify that EU cyber security policy did not alter, but became more entrenched as a result of these incidents. This is an area of potential future research in HI scholarship.

The thesis's adoption of an HI approach also contributed to the general understanding of the EU beyond cyber security policy. By encouraging a more longitudinal approach the analysis of policy decisions need not be restricted to specific points in time, or considered as a response to single, major events. As the analysis of cyber security has shown, EU policy can develop as a response to a series of events and decisions taken over a long period of time. In the case of cyber security this was 28 years. A more nuanced understanding of EU policy in any sector can be achieved if this longitudinal approach is adopted. This thesis therefore makes a substantive contribution to current scholarship and, it is hoped, can provide a link to new and equally dynamic areas of examination in cyber security and beyond the EU.

Cyber security itself promises to be a fruitful and rewarding research field. At the time of writing the EU is currently undergoing major changes and demonstrating a resurgence of confidence in defence matters. Analysts are commenting that defence integration is set to progress (Kern, 2016) and that the French and German governments are discussing the initiation of a dedicated EU army (Kornelius, 2016). Such developments in defence policy raise the prospect of the development of a more defence-oriented cyber security policy. The evidence gathered for this thesis would suggest, however, that EU cyber security policy will continue on established, long-term, socio-economic policy paths.

This is not a prediction of future development. EU cyber security policy has shown itself to be highly resilient to change, even in the face of major structural changes to the EU itself. Cyber security policy has remained on socio-economic paths founded upon five core elements for nearly 30 years. Even after the entry into force of the Treaty of Lisbon, which radically altered the structure of the EU itself, policy in this sector continued unchanged. There is therefore nothing to suggest that a new-found defence confidence will lead to a more defence-oriented approach to cyber security. One reason for this is that Union competences have not changed. The EU remains restricted in its capacity to act and will continue to be so unless a substantial change to Union competences occurs to expand them beyond their socio-economic boundaries.

That being the case, EU cyber security policy has taken unexpected paths in the past. The EU maintained a socio-economic approach when other actors added defence- or national

security-oriented paradigms. The EU's policy approach has not changed even when such a change is expected to occur in response to major events. Given the current developments in EU defence policy, a harder approach to cyber security will not be a surprising development. Cyber security is a dynamic, constantly shifting subject and the EU's responses to this ever-changing field will provide fruitful and interesting research in the future.

Appendices

Appendix 1 – European policy and legislative documents relevant for cyber security

The European policy documents relevant for cybersecurity include:

- The Commission Communication on "Network and Information Security: Proposal for A European Policy Approach"[65] of 2001.
- The establishment of the European Network and Information Security Agency (ENISA)[66] in 2004.
- The Commission Communication on a "Strategy for a Secure Information Society - Dialogue, partnership and empowerment"[67] of 2006.
- The Commission Communication on a "European Programme for Critical Infrastructure Protection (EPCIP)" [68] of 2006 which sets forth the horizontal framework for the protection of critical infrastructures in the EU.
- The Safer Internet Programme[69] 2009-2013 adopted in 2008 to promote safer use of the Internet and other communication technologies, particularly for children, and to fight against illegal content and harmful conduct online.
- The Communication on Critical Information Infrastructure protection (CIIP)[70] of 2009 focusing on the protection of Europe from cyber-attacks and cyber disruptions by enhancing preparedness, security and resilience and launching an action plan with five pillars of actions: preparedness and prevention; detection and response; mitigation and recovery; international cooperation; criteria for the ICT sector.
- Directive 2009/140/EC of the European Parliament and of the Council amending Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive)[71] which sets new provisions on security and integrity of networks and services (Art. 13 a and b of Framework Directive).
- The Trust and Security chapter of the Digital Agenda for Europe[72], which launched several action addressing security and resilience.
- The Commission proposal to modernise the European Network and Information Security Agency (ENISA), which is currently under discussion in the Council and the European Parliament[73].
- The Stockholm Programme/Action Plan[74] and the EU Internal Security Strategy in action[75] (ISS) which underline the Commission's commitment to building a digital

[65] COM(2001) 298 http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf
[66] See Regulation (EC) No 460/2004 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=-CELEX:32004R0460:EN:HTML and
[67] COM(2006)251 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf
[68] COM(2006)786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf
[69] Decision No 1351/2008/EC http://ec.europa.eu/information_society/activities/sip/docs/prog_decision_2009/decision_en.pdf
[70] COM(2009)149 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
[71] See http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf
[72] COM(2010)245 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF
[73] COM(2010)521 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF
[74] COM(2010)171 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF

environment where every European can fully express his or her economic and social potential.

- The second Commission Communication on CIIP of March 2011[76] on 'Achievements and next steps: towards global cyber-security' which take stock of the results achieved since the adoption of the CIIP action plan in 2009 and describe the next priorities planned under each action at both European and international level.
- The Commission proposals on a Directive on attacks against information systems and the Directive 2011/92/EU[77] on combating the sexual abuse and sexual exploitation of children and child pornography adopted on 1st December 2011.
- 2013 Cyber Security Strategy.
- 2013 proposed directive concerning measures to ensure a high common level of network and information security across the Union.

[75] COM(2010)673 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF
[76] COM(2011)163 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF
[77] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF

Appendix 2 – EU Acquis relevant to Cyber Security

Acquis Document Name	*Nodes*	*References*
Bangemann Report to European Council May 1994	18	36
COM (1985) 310_f_en Completing the internal market	8	27
COM (1992) 24 final Proposal for a Council Directive on the legal protection of databases	3	5
COM (1992) 422 final Proposal for a council directive on protection of processing personal data	2	2
COM (1993) 700 Commission White paper Growth, Competitiveness, Employment: The challenges	16	51
COM (1994) 347 Information Society Action Plan	14	40
COM (1995) 492 final REPORT FROM THE COMMISSION on the main events and developments of the info market 1993-4	15	44
COM (1996) 389 final Green Paper living and working in the information society	9	32
COM (1996) 395 final Info society impact on EU policies	15	23
COM (1996) 471 final Learning in the information society: plan for education initiative	9	13
COM (1996) 483 Green Paper on the protection of minors and human dignity in audio-visual and info services	10	26
COM (1996) 487 final Illegal and harmful content on the Internet	18	43
COM (1996) 607 final Europe at the forefront of the information society	5	6
COM (1997) 157 initiative on electronic commerce	10	30
COM (1997) 503 Ensuring security and trust in electronic communications	15	31
COM (1997) 582 final Action plan on promoting safe use of the Internet	13	32
COM (1998) 50 final need for Strengthened international coordination	7	11
COM (2000) 130 eEUROPE	2	3
COM (2000) 890 computer related crime	23	77
COM (2001) 140 eEurope impact and priorities	2	3
COM (2001) 298 network and info security proposal for a European policy approach	16	23

COM (2005) 229 FINAL "i2010 – A European Information Society for growth and employment"	17	38
COM (2005) 576 en 01 GREEN PAPER on a European program for critical infrastructure protection	1	1
COM (2006) 251 A strategy for a Secure Information Society – Dialogue, partnership and empowerment	15	26
COM (2006) 786 COMMUNICATION FROM THE COMMISSION on a European Programme for	3	4
COM (2007) 267 towards a policy on cybercrime	11	16
COM (2008) 712 legislative and work programme vol. 1 final	4	4
COM (2009) 149 CIIP Protecting Europe from large scale cyber-attacks and disruptions enhancing resilience	16	23
COM (2009) 277 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Internet governance the next steps	8	8
COM (2009) 324 final ICT Standardisation	2	2
COM (2010) 171 final Stockholm program	13	20
COM (2010) 245 digital-agenda for Europe-communication-en	20	34
COM (2010) 517 proposal for a directive on attacks on info systems	12	20
COM (2010) 521 proposal for a regulation concerning ENISA	17	32
COM (2010) 608 final2 proposals for a single market	9	14
COM (2010) 673 final EU internal security strategy	8	14
COM (2011) 163 final Communication on Critical Info Infra protection - achievements and next steps towards global cyber security	16	30
COM (2011) 522 proposal for a regulation on co-operation through IMI	8	22
COM (2011) 566 final Report from Commission Protecting Children in digital world	4	5
COM (2011) 60 final EU agenda on rights of the child	1	1
COM (2011) European principles and guidelines on internet resilience	21	30
COM (2012) 140 final establishing a European Cybercrime centre	15	23
COM (2012) 196 Final European Strategy for a Better Internet for Children	16	23
COM (2013) 48 final Proposal for a DIRECTIVE OF THE EUROPEAN	24	64

PARLIAMENT AND OF THE COUNCIL		
Council of EU 2009 European Security Strategy	6	6
Council of EU 2011 April Hungary: CIIP Conference Presidency Statement	9	12
Council of EU 2012 Dec Friends of the Presidency Group on Cyber Issues	1	1
Council of EU Conclusions 1997 March on harmful content of internet	6	12
Council of EU Conclusions 1999 Dec 14th Protection of minors	4	7
Council of EU Conclusions 1999 May 23rd Brussels Budapest convention	6	6
Council of EU Conclusions 1999 Sept 16th Digital TV and protection of Minors	1	1
Council of EU Conclusions 2001 May Brussels CIIP	14	18
Council of EU Conclusions 2001 Nov 18th Spain's view on Europol cyber-crime centre	11	16
Council of EU Conclusions 2002 Jan Establishing a cyber-crime centre at Europol	5	5
Council of EU Conclusions 2002 May 13th Brussels preserving digital culture	4	4
Council of EU Conclusions 2003 Nov 7th Digital content	7	9
Council of EU Conclusions 2004 May 14 Accessible Digital Content	12	23
Council of EU Conclusions 2007 8th November general inc. cyber-crime	5	8
Council of EU Conclusions 2007 March 23 CIIP	4	5
Council of EU Conclusions 2008 July 11 Plan to combat cyber-crime	8	11
Council of EU Conclusions 2009 Dec Resolution on collaborative approach to NIS	13	18
Council of EU Conclusions 2009 July 22 Position of Netherlands on cyber-crime	8	12
Council of EU Conclusions 2010 May 26 Adoption of resolution on Digital agenda	9	17
Council of EU Conclusions 2011 April 8 CIIP	10	13
Council of EU Conclusions 2011 December Brussels (open internet)	6	9

Council of EU Conclusions 2011 May 19th CIIP and cyber security	8	9
Council of EU Conclusions 2011 Nov 28 terrorist cyber-attacks	7	11
Council of EU Conclusions 2011 Nov Brussels children in digital world	7	8
Council of EU Conclusions 2012 Dec 5th PRESS RELEASE Launch of Global alliance against child sexual exploitation	3	3
Council of EU Conclusions 2012 Nov 21 Record of Parliament discussions on CSDP	5	5
Council of EU Conclusions 2012 Nov 6th Better coordination in council on cyber policy issues	11	15
Council of EU Conclusions 2013 July Brussels conclusions on cyber security strategy	17	29
Council of EU Conclusions 2013 Luxembourg approving Cybersecurity Strategy	25	55
Council of EU Conclusions 2013 Nov 26th Draft operational action plan on cyber-attacks	2	2
Council of EU Conclusions 2013 Nov 5th COREPER report on FoP activities	5	6
Council of EU Conclusions 2013 November Brussels CSDP	6	7
Council of EU Conclusions 2013 Sept joint debate with EP cyber security digital agenda	8	13
Council of EU Policy Outline 2013 Feb 7 Improving cyber security across the EU - Policy outline	5	5
Council of EU Resolution 2009 Dec 29 on a collaborative European approach to Network and Information Security	12	21
Decision 1992 March of the Council on security of information systems	7	7
DECISION 1999 No 276 1999 EC promoting safer use of the interne	10	19
Decision 2000 375 on child pornography	7	13
DECISION 2005 COUNCIL FRAMEWORK DECISION 222 JHA of 24 Feb 2005 on attacks against info systems	7	10
DECISION 2008 No 1351 EC Child protection on the internet	8	17
Decision 2013 Dec 3rd of the Council establishing programme implementing H2020	15	30
Directive 1990 388 of the Commission EEC 28 June 1990 on competition in the markets for telecoms services CELEX_31990L0388_EN_TXT	3	4

Directive 1991 250 EEC of the Council MAY 1991 ON LEGAL PROTECTION OF COMPUTER PROGRAMMS	4	4
Directive 1995 46 EC Parliament and Council on protection of individuals regarding processing of personal data	3	11
Directive 1996 9 EC 11 March 1996 on legal protection of databases	3	3
Directive 1997 66 EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 15 Dec 1997 concerning the processing of personal data and protection of privacy	3	9
Directive 1999 93 EC Parliament and Council on electronic signatures REPEALED REPLACED 2014	2	5
Directive 2000 31 EC of the European Parliament and of the Council of 8 June 2000 Directive on electronic commerce	9	33
Directive 2002 19 EC Access Directive	1	1
Directive 2002 21 EC regulatory framework for electronic communications networks	6	9
Directive 2002 58 EC data protection	3	5
Directive 2008 114 EC of the Council identification and designation of European critical infrastructure	6	8
Directive 2009 140 EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL On Electronic communications	8	12
Directive 2011 92 EU on child pornography	4	4
European Council Conclusions 1992 Dec Edinburgh	1	1
European Council Conclusions 1993 December Brussels	2	2
European Council Conclusions 1993 June Copenhagen	4	5
European Council Conclusions 1994 Dec Essen	8	8
European Council Conclusions 1994 June Corfu	9	14
European Council Conclusions 1998 Dec Vienna	5	7
European Council Conclusions 1999 Dec Helsinki	6	9
European Council Conclusions 1999 June Cologne	8	14
European Council Conclusions 2000 March Lisbon	5	6
European Council Conclusions 2001 March Stockholm	5	5
European Council Conclusions 2002 March Barcelona	5	7

European Council Conclusions 2003 March Brussels	6	10
European Council Conclusions 2003 Oct Brussels	1	2
European Council Conclusions 2004 November Brussels	2	2
European Council Conclusions 2006 December Brussels	1	1
European Council Conclusions 2006 June Brussels	3	3
European Council Conclusions 2006 March Brussels	3	4
European Council Conclusions 2007 December Brussels	3	4
European Council Conclusions 2008 December Brussels	2	2
European Council Conclusions 2008 June Brussels	2	2
European Council Conclusions 2009 March Brussels	3	3
European Council Conclusions 2010 June	2	2
European Council Conclusions 2010 September	2	2
European Council Conclusions 2011 December	2	2
European Council Conclusions 2011 October	2	2
European Council Conclusions 2012 June	4	6
European Council Conclusions 2012 March	1	1
European Council Conclusions 2012 October	3	4
European Council Conclusions 2013 Dec Brussels	3	4
European Council Conclusions 2013 Oct Brussels	6	8
JOIN (2013) 1 final Cybersecurity Strategy of the EU	42	128
PRESS RELEASE Council Conclusions 5 Dec 2012 Launch of Global alliance against child sexual exploitation	3	4
Regulation (EC) 2004 No 460 2004 establishing ENISA	9	15
Regulation (EU) 2012 No 1024 of 25 Oct 2012 on administering co-operation through the IMI	3	9
Regulation (EU) 2013 No 1291 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2013 establishing Horizon 2020	14	28
Regulation (EU) 2013 No 526 Concerning ENISA and repealing Regulation (EC) 460 2004	13	19

SEC (2006) 642 cyber-crime impact	8	11
SEC (2010) 1123_EN impact assessment re repealing 2005 directive	10	19
Treaty 1987 Single European Act establishing the European Communities	5	12
Treaty 1992 Maastricht Treaty on European Union	4	9
Treaty 1997 Amsterdam c_34019971110en	8	20
Treaty 2001 Nice Establishing the European Community	4	6
Treaty 2009 European Union AND Treaty on the Functioning of the EU CONSOLIDATED	9	14
Treaty 2009 Lisbon amending the Treaty on European Union and the Treaty establishing the European Community 2007	4	6
Treaty 2010 Charter of Fundamental Rights of the European Union	1	1

Appendix 3 – Acquis categorised by Actor and Publication Date

Year	Commission	Euco	CoEU	Directives	Decisions	Regulations	Treaties	Historic events
1985	COM (1985) 310_f_en Completing the internal market (includes info tech and info sharing) CODED							
1987							Treaty 1987 Single European Act establishing_the_european_communities CODED	
1990	Directive 1990 388 of the Commission EEC 28 june 1990 on competition in the markets for telecoms services CELEX_31990L0388_EN_TXT CODED			Directive 1991 250 eec of the Council MAY 1991 ON LEGAL PROTECTION OF COMPUTER PROGRAMMS CODED Z				
1992	COM (1992) 24 final Proposal for a Council Directive on the legal protection of databases CODED COM (1992) 422 final Proposal for a council directive on protection of processing personal data UNI PITT ARCHIVE 130 PAGES	European Council Conclusions 1992 Dec Edinburgh CODED Z			Decision 1992 March of the Council on security of information systemsCELEX-31992D0242-EN-TXT CODED		Treaty 1992 Maastricht Treaty_on_european_union CODED First mention of EC "competence"	Establishment of Single Market
1993	COM (1993) 700 Commission White paper Growth, Competitiveness, Employment The challenges NVIVO CODED	European Council Conclusions 1993 December Brussels CODED Z European Council Conclusions 1993 June Copenhagen CODED Z						
1994	Bangemann Report to European Council May 1994 Z COM (1994) 347 info_socieity_action_plan_PPP CODED	European Council Conclusions 1994 Dec Essen European Council Conclusions 1994 June Corfu CODED Z						
1995	COM (1995) 492 final REPORT FROM THE COMMISSION on the main events and developments of the info market 1993-4 CODED			Directive 1995 46 EC Parl and Council on protection of individuals regarding processing of personal data CODED				

Year	Commission	Euco	CoEU	Directives	Decisions	Regulations	Treaties	Historic events
1996	COM (1996) 389 final Green Paper living and working in the information society CODED COM (1996) 395 final Info society impact on EU policies CODED COM (1996) 471 final Learning in the information society plan for education initiative CODED COM (1996) 483 Green Paper on the protection of minors and human dignity in audiovisual and info services CODED COM (1996) 487 final Illegal and harmful content on the Internet PPP CODED COM (1996) 607 final Europe at the forefront of the information society CODED			Directive 1996 9 EC 11 March 1996 on legal protection of databases CELEX_31996L0009_EN_TXT 4 yrs after COM proposal CODED				
1997	COM (1997) 157 initiative on electronic commerce CODED Z COM (1997) 503 Ensuring security and trust in electronic comms CODED COM (1997) 582 final Action plan on promoting safe use of the Internet PPP CODED		Council of EU Conclusions 1997 March on harmful content of internet CODED	Directive 1997 66 EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 15 Dec 1997 concerning the processing of personal data and protection of privacy CODED			Treaty 1997 Amsterdam c_34019971110en CODED	
1998	COM (1998) 50 final need for Strengthened intl coordination CODED	European Council Conclusions 1998 Dec Vienna CODED Z						

Year	Commission	Euco	CoEU	Directives	Decisions	Regulations	Treaties	Historic events
1999		European Council Conclusions 1999 June Cologne CODED Z	Council of EU Conclusions 1999 Dec 14th Protection of minors CODED	Directive 1999 93 EC Parl and Council on electronic signatures REPEALED REPLACED 2014 CODED Z	DECISION 1999 No 276 1999 EC promoting safer use of the internet CELEX_31999D0276_EN_TXT CODED Z			
		European Council Conclusions 1999 Helsinki CODED Z	Council of EU Conclusions 1999 May 23rd Brussels Budapest convention CODED Council of EU Conclusions 1999 Sept 16th Digitla TV and protection of Minors CODED					
2000	COM (2000) 130 eEUROPE CODED	European Council Conclusions 2000 March Lisbon CODED Z		Directive 2000 31 EC of the European Parliament and of the Council of 8 June 2000 Directive on electronic commerce CODED Z	Decision 2000 375 On_child_pornography_en_1 CODED Z			
	COM (2000) 890 computer related crime CODED							
2001	COM (2001) 140 eEurope impact and priorities	European Council Conclusions 2001 March Stockholm CODED Z					Treaty 2001 Nice Establishing the European CommunityEIF 1_2_2003 CELEX_12002E_TXT_EN_TXT CODED	
	COM (2001) 298 network and info security proposal for a European policy approach PPP CODED DEVELOPED IN RESPONSE TO COLOGNE EUCO 1999		Council of EU Conclusions 2001 Nov 18th Spain's view on Europol cyber crime centre CODED					

Year	Commission	Euco	CoEU	Directives	Decisions	Regulations	Treaties	Historic events
2002		European Council Conclusions 2002 March Barcelona CODED Z	Council of EU Conclusions 2002 Jan CIIP Info net security est cyber crime cenre at Europol CODED Council of EU Intro note from PermRep to Council 2002 May 13th Brussels preserving digital culture CODED	Directive 2002 19 EC Access Directive CODED Directive 2002 21 EC regulatory framework for elec comms networks CODED Directive 2002 58 EC data protection CODED				
2003		European Council Conclusions 2003 March Brussels CODED Z European Council Conclusions 2003 Oct Brussels CODED Z	Council of EU Conclusions 2003 Nov 7th Note from Presidency to Council Digital content CODED					
2004		European Council Conclusions 2004 November Brussels CODED Z	Council of EU Conclusions 2004 May 14 Accessible Digital Content CODED			Regulation (EC) 2004 No 460 2004 establishing ENISA CODED Z		
2005	COM (2005) 229 FINAL "i2010 – A European Information Society for growth and employment" CODED COM (2005) 576 en 01 GREEN PAPER on a european program for ciritical infrastructure protection CODED				DECISION 2005 COUNCIL FRAMEWORK DECISION 222 JHA of 24 feb 2005 on attacks against info systems CODED			
2006	COM (2006) 251 A strategy for a Secure Information Society – Dialogue, partnership and PPPNVIVO CODED COM (2006) 786 COMMUNICATION FROM THE COMMISSION on a European Programe for CIP CODED	European Council Conclusions 2006 December Brussels CODED Z European Council Conclusions 2006 June Brussels CODED Z European Council Conclusions 2006 March Brussels CODED Z						

Year	Commission	Euco	CoEU	Directives	Decisions	Regulations	Treaties	Historic events
2007	COM (2007) 267 towards a policy on cybercrime CODED SEC (2007) 642 Commission staff working document cyber crime impact CODED	European Council Conclusions 2007 December Brussels CODED Z	Council of EU Conclusions 2007 8th November general inc cyber crime CODED Council of EU Conclusions 2007 March 23 CIIP CODED					Estonian cyber attack
2008	COM (2008) 712 legislative and work programme vol Ifinal CODED	European Council Conclusions 2008 December Brussels CODED Z European Council Conclusions 2008 June Brussels CODED Z	Council of EU Conclusions 2008 July 11 Plan to combat cyber crime CODED	Directive 2008 114 EC of the Council identification and designation of european critical infrastructure CODED	DECISION 2008 No 1351 EC Child protection on the internet CODED			Georgian cyber attack
2009	COM (2009) 149 CIIP Protecting Europe from large scale cyber-attacks and disruptions enhancing resilience CODED COM (2009) 277 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Internet governance the next steps CODED COM (2009) 324 final ict standardisation CODED AN EXAMPLE OF A POLICY WHICH SHARES A NUMBER OF KEY PRINCIPLES BUT IS NOT STRICTLY RELATED TO CYBER SECURITY, ONLY TANGENTIALLY	European Council Conclusions 2009 March Brussels CODED Z	Council of EU 2009 European Security Strategy CODED Council of EU Conclusions 2009 Dec Resolution on collaborative approach to NIS CODED Council of EU Conclusions 2009 July 22 Position of Netherlands on cyber crime CODED Council of EU Resolution 2009 Dec 29 on a collaborative European approach to Network and Information Security CODED	Directive 2009 140 EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Electronic communications CODED			Treaty 2009 European Union AND Treaty on the Functioning of the EU CONSOLIDATED Treaty 2009 Lisbon amending the Treaty on European Union and the Treaty	
2010	COM (2010) 171 final stockholm program CODED COM (2010) 245 digital-agenda for europe-communication-en CODED COM (2010) 517 proposal for a directive on attacks on info systems CODED COM (2010) 521 proposal for a regulation concerning ENISA CODED COM (2010) 608 final2 proposals for a single market CODED COM (2010) 673 final EU internal security strategy CODED SEC (2010) 1123_EN impact assessment re relealing 2005 directive CODED	European Council Conclusions 2010 June CODED Z European Council Conclusions 2010 September CODED Z	Council of EU Conclusions 2010 May 26 Adoption of resolution on Digital agenda CODED				Treaty 2010 Charter of Fundamental Rights of the Europena Union c_326 20121026en03910 407 CODED	Stuxnet

Year	Commission	Euco	CoEU	Directives	Decisions	Regulations	Treaties	Historic events
2011	COM (2011) 163 final Comm on Critical Info Infra protection - achievements and next steps towards global cyber security CODED	European Council Conclusions 2011 December CODED Z	Council of EU 2011 April HU_CIIP_Conference_Presidency_Statement_final CODED	Directive 2011 92 EU on child pornography CODED				
	COM (2011) 522 proposal for a regulation on co-operation through IMI CODED	European Council Conclusions 2011 October CODED Z	Council of EU Conclusions 2011 April 8 CIIP CODED					
	COM (2011) 566 final Report from Commission Protecting Children in digital world CODED		Council of EU Conclusions 2011 December Brussels (open internet) CODED					
	COM (2011) 60 final EU agenda on rights of the child CODED		Council of EU Conclusions 2011 May 19th CIIP and cyber security CODED					
	COM (2011) European principles and guidelines on internet resilience CODED		Council of EU Conclusions 2011 27 May Brussels CIIP CODED					
			Council of EU Conclusions 2011 Nov 28 terrorist cyber attacks CODED					
			Council of EU Conclusions 2011 Nov Brussels children in digital world CODED					
2012	COM (2012) 140 final establishing a European Cybercrime centre CODED	European Council Conclusions 2012 June CODED Z	Council of EU 2012 Dec FoP Agenda CODED			Regulation (EU) 2012 No 1024 of 25_10_2012 on admin co-op through IMI		
	COM (2012) 196 Final European Strategy for a Better Internet for Children CODED	European Council Conclusions 2012 March CODED Z	Council of EU Conclusions 2012 Dec 5th PRESS RELEASE Launch of Global alliance against child sexual exploitation CODED			STATES COMMISSION PROVIDES SECURITY CODED		
		European Council Conclusions 2012 October CODED Z	Council of EU Conclusions 2012 Nov 21 Record of Parliament discussions on CSDP CODED					
			Council of EU Conclusions 2012 Nov 6th Better coordination in council on cyber policy issues CODED					
			PRESS RELEASE Council Conclusions 5 Dec 2012 Launch of Global alliance against child sexual exploitation CODED					

Year	Commission	Euco	CoEU	Directives	Decisions	Regulations	Treaties	Historic events
2013	COM (2013) 48 final Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL CODED	European Council Conclusions 2013 Dec Brussels CODED Z	Council of EU Conclusions 2013 July Brussels conclusions on cy sec strat CODED		Decision 2013 Dec 3rd of the Council establishing programme implementing H2020 CODED	Regulation (EU) 2013 No 1291 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2013 establishing Horizon 2020 CODED		
	JOIN (2013) 1 final Cybersecurity Strategy of the EU CODE	European Council Conclusions 2013 Oct Brussels CODED Z	Council of EU Conclusions 2013 Luxembourg approving Cybersecurity Strategy CODED			Regulation (EU) 2013 No 526 Concerning EnISA and repealing Regulation (EC) 460 2004 CODED Z		
			Council of EU Conclusions 2013 Nov 26th Draft operational action plan on cyber attacks CODED					
			Council of EU Conclusions 2013 Nov 5th COREPER report on FoP activities CODED					
			Council of EU Conclusions 2013 November Brussels CSDP CODED					
			Council of EU Conclusions 2013 Sept joint debate with EP cyber security digital agenda CODED					
			Council of EU Policy Outline 2013 Feb 7 Improving cyber security acros the EU - Policy outline CODED					

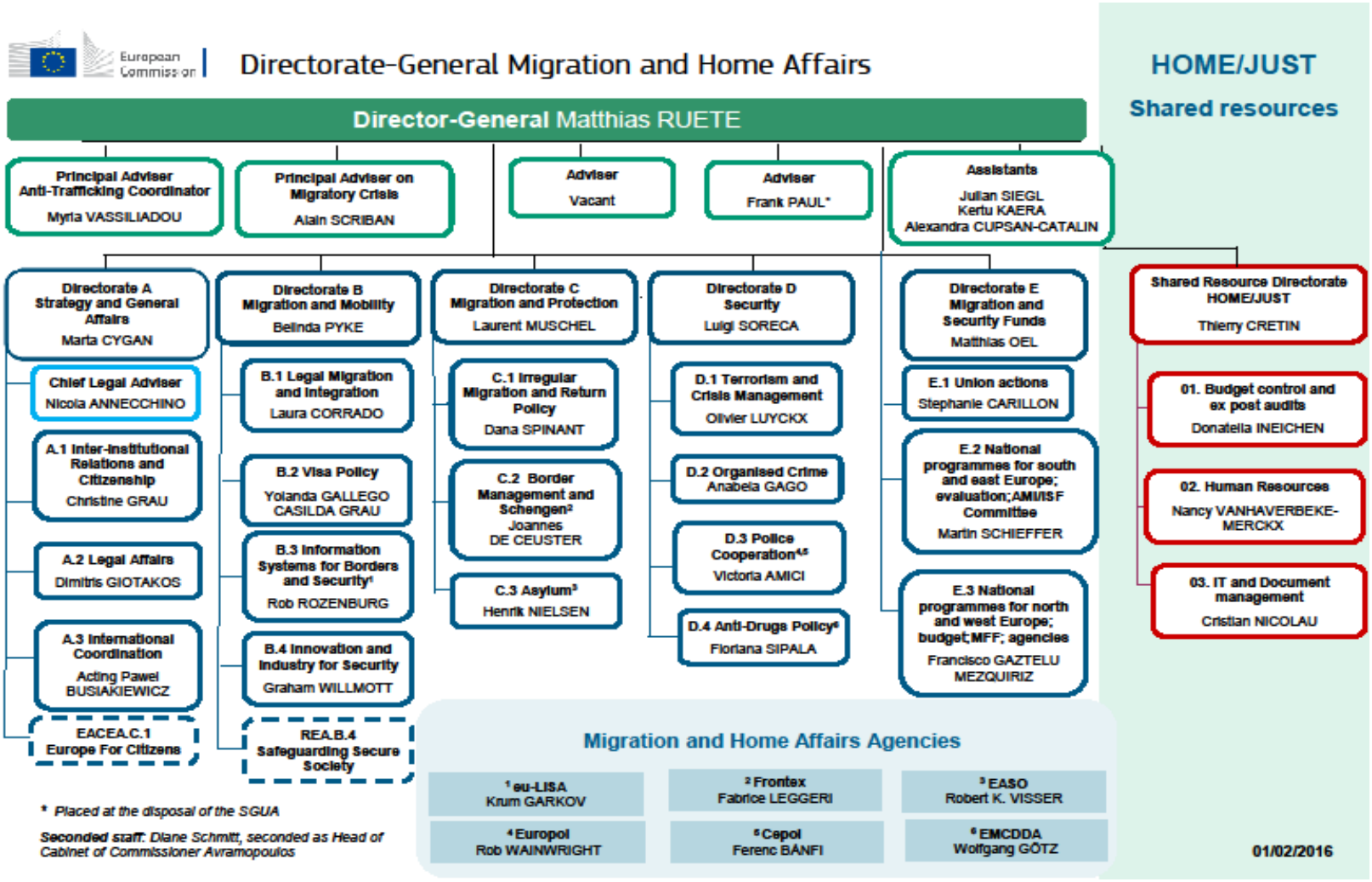
Appendix 4 – EU *acquis* relating to Critical Information Infrastructure Protection

Acquis Document Name	References
COM (2005) 229 FINAL i2010 – A European Information Society for growth and employment	1
COM (2005) 576 en 01 GREEN PAPER on a European program for critical infrastructure protection	1
COM (2007) 267 towards a policy on cybercrime	1
COM (2009) 149 CIIP Protecting Europe from large scale cyber-attacks and disruptions enhancing resilience	1
COM (2009) 277 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Internet governance the next steps	1
COM (2010) 245 digital agenda for Europe	1
COM (2010) 517 proposal for a directive on attacks on info systems	1
COM (2011) 163 final Communication on Critical Info Infra protection - achievements and next steps towards global cyber security	1
COM (2011) European principles and guidelines on internet resilience	1
COM (2013) 48 final Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	3
Council of EU 2009 European Security Strategy	1
Council of EU 2011 April Hungary: CIIP Conference Presidency Statement	1
Council of EU Conclusions 2009 Dec Resolution on collaborative approach to NIS	1
Council of EU Conclusions 2011 April 8 CIIP	1
Council of EU Conclusions 2011 May 19th CIIP and cyber security	1
Council of EU Conclusions 2011 May Brussels CIIP	1
Council of EU Conclusions 2011 Nov 28 terrorist cyber-attacks	1
Council of EU Conclusions 2012 Nov 6th Better coordination in council on cyber policy issues	1
Council of EU Conclusions 2013 July Brussels conclusions on the Cyber Security Strategy	2
Council of EU Conclusions 2013 Luxembourg approving Cybersecurity Strategy	1
Decision 2013 Dec 3rd of the Council establishing programme implementing H2020	2
European Council Conclusions 2001 March Stockholm	1
JOIN (2013) 1 final Cybersecurity Strategy of the EU	1

Appendix 5 – EU *acquis* relating to the 2008 financial crisis

Acquis Document Name	References
COM (2008) 712 legislative and work programme vol. 1 final	9
COM (2009) 277 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Internet governance the next steps	1
COM (2010) 171 final Stockholm program	2
COM (2010) 608 final2 proposals for a single market	4
Council of EU Conclusions 2011 December Brussels (open internet)	1
Council of EU Conclusions 2012 Nov 21 Record of Parliament discussions on CSDP	1
Council of EU Conclusions 2013 November Brussels CSDP	1
Decision 2013 Dec 3rd of the Council establishing programme implementing H2020	1
European Council Conclusions 1998 Dec Vienna	1
European Council Conclusions 2008 December Brussels	2
European Council Conclusions 2009 March Brussels	1
European Council Conclusions 2010 June	1
European Council Conclusions 2010 September	1
European Council Conclusions 2011 December	1
European Council Conclusions 2011 October	1
Regulation (EU) 2013 No 1291 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2013 establishing Horizon 2020	3

Appendix 6 – European Commission DG HOME Organisation Chart



Appendix 7 – Sample Interview Questions

Sample questions

(Not all questions will be relevant for all participants)

1. What have been the most important factors in the development of the European Union (EU)'s response to cybersecurity challenges?

2. A hypothesis of this research project is that, as a result of a number of institutional forces, the EU approaches the problem of cybersecurity from a socio-economic, criminal justice, standpoint in contrast to the more military approaches of other actors in the field. What is your opinion on this hypothesis?

3. A second hypothesis of this research project is that there is an historic correlation between the EU's cybersecurity policy and its wider foreign and security policy (CFSP). What is your opinion on this hypothesis?

4. It was stated in the EU's 2013 Cybersecurity Strategy that "dealing with security challenges in cyberspace is predominantly the task of Member States." If this is the case, what are the reasons behind the EU becoming involved in cybersecurity to the extent that it has done, with the initiation of eu-LISA, ENISA and the European Cyber-Crime Centre at Europol?

5. If the EU has restricted competence in security matters, and exclusive or shared competence in certain socio-economic policy areas, can the EU's 2013 Cybersecurity Strategy and Directive be seen as an attempt to combine its competences between these areas?

6. A goal cited in the 2013 Cybersecurity Strategy is the development of cyber defence capabilities. What can EU do or achieve in this area given that defence remains a national remit?
    a. Is the EU attempting to build a capacity alongside national defence strategies and capabilities?

7. Coherence in cybersecurity responses is also cited as a goal for the EU. How can the EU achieve this given that much of the infrastructure on which cyberspace is based is owned and operated by global private actors, many of whose headquarters are not located within EU geopolitical borders?

8. What has been the impact of the Treaty of Lisbon on EU cybersecurity?

9. What is your view on the role of the Friends of the Presidency Group on Cyber Issues?

Appendix 8 – Participant Information and Plain Language Statement

University of Glasgow | College of Social Sciences

Plain Language Statement

1. Study title and Researcher Details

Cyber Security and the European Union: An Historical Institutionalist Analysis of a 21st Century Security Concern

Researcher: Robert S. Dewar

2. Invitation paragraph

You are being invited to take part in a research study. Before you decide it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or if you would like more information. Take time to decide whether or not you wish to take part.

Thank you for reading this.

3. What is the purpose of the study?

To examine the response of the European Union to Cyber Security issues, and apply Institutionalist principles to that examination.

4. Why have I been chosen?

Your participation in this study has been requested because your expertise and experience in the field of European cyber security would be valuable to the development of this research project.

5. Do I have to take part?

No. Participation is entirely voluntary.

6. What will happen to me if I take part?

Your participation is entirely voluntary. Should you consent to be identified in the final dissertation, you will be named as a source in the bibliography. Should you choose to participate anonymously, no identification will be made.

Should you choose to participate in this research project you will be asked for an interview regarding your involvement and views on the subject of the project. The interview will last approximately 1 to 1.5 hours.

The interviews will be held face-to-face in person at a time and location convenient to you. Should a face-to-face meeting not be feasible or appropriate, the interviews may be conducted by telephone, video-conferencing (e.g. Skype) or via email exchange, whichever is most suitable for you.

A set of preliminary questions will be provided in advance of the interview. This will demonstrate the subject areas which the researcher wishes to discuss, based on your expertise. During the course of the interview other questions may arise as a consequence of themes under discussion.

The interviews will be audiotaped, but only if you consent to this. Question 3 of the accompanying Consent Form enables you to provide or deny consent for interviews to be audiotaped.

During the interview you have the right at any time to withdraw an answer, refuse to answer a question or end the interview. Participation in this research study and the answering of any specific question is entirely voluntary.

7. Will my taking part in this study be kept confidential?

Yes. There is a section on the participation consent form which allows you to state at what level you would prefer to participate. You can choose to be named in the final thesis or, should you not wish to be named, you may choose to participate under a pseudonym so that you cannot be identified. Alternatively you may choose to have your input to this project attributed to the institution you represent, with no name or pseudonym assigned in the study.

8. What will happen to the results of the research study?

The results will be analysed and submitted in a PhD thesis for the University of Glasgow. Should you choose to participate a written summary of the results of the research study will be provided to you.

9. Who is organising and funding the research? (If relevant)

This is an independent piece of research for a PhD thesis at the University of Glasgow.

Fieldwork funding is being provided by the University Association for Contemporary European Studies.

10. Who has reviewed the study?

The study has been reviewed by the College of Social Sciences Ethics Committee and is being supervised by Dr Brandon Valeriano and Dr Eamonn Butler of the University of Glasgow.

11. Contact for Further Information

If you would like further clarification or information, Please contact the researcher, Robert Dewar. He can be contacted at

Email: r.dewar.1@research.gla.ac.uk

If you have any concerns regarding the conduct of the research project that they can contact the College of Social Sciences Ethics Officer by contacting Dr Valentina Bold, (valentina.bold@glasgow.ac.uk)

http://www.gla.ac.uk/colleges/socialsciences/info/students/ethics/committee/

Appendix 9 – Sample Participant Consent Form

University of Glasgow | College of Social Sciences

Consent Form

Title of Project: Cyber Security and the European Union: An Historical Institutionalist Analysis of a 21st Century Security Concern

Name of Researcher: Robert S. Dewar

1. I confirm that I have read and understand the Plain Language Statement for the above study and have had the opportunity to ask questions.

2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.

3. I consent to the interview being audio-taped

   Yes

   No

   (Please delete as applicable)

4. I agree to be identified in any publications arising from the research via the following:

   a) By name
   b) Via a pseudonym which will be assigned by the researcher
   c) By institution only
   (Please delete as applicable

5. I understand that copies of the interview transcripts may be returned to me for verification if I request this.

6. I agree / do not agree (delete as applicable) to take part in the above study.

Name of Participant	Date	Signature
Researcher	Date	Signature

1 for subject; 1 for researcher

Appendix 10 – List of Referable Interview Participants

Names of Interviewees are provided where permission was given to do so.

Organisation	***Name***	***Location***	***Date***
	European Union		
European Network and Information Security Agency	Dr Steve Purser	Athens, Greece	14/05/2014
European Network and Information Security Agency	Prof. Dr. Udo Helmbrecht	Heraklion, Greece	16/05/2014
Europol		The Hague, Netherlands	22/05/2014
European Cyber Crime Centre		The Hague, Netherlands	23/05/2014
eu-LISA		Tallinn, Estonia	28/05/2014
European Defence Agency	Wolfgang Roehrig	Brussels, Belgium	11/06/2014
European External Action Service		Brussels, Belgium	11/06/2014
DG Connect, European Commission		Brussels, Belgium	12/06/2014
DG MARKT, European Commission		Brussels, Belgium	13/06/2014
CERT-EU		Brussels, Belgium	17/06/2014
European Parliament		Brussels, Belgium	17/06/2014
European Union		Brussels	17/06/2014
Bureau of European Policy Analysis, European Commission		Brussels, Belgium	19/06/2014
DG HOME, European Commission		Brussels, Belgium	19/06/2014
EPP, European Parliament	Tunne Kelam, MEP	Brussels, Belgium (Telephone)	08/07/2014
DG Connect, European Commission	Ann-Sofie Rönnlund	Brussels, Belgium	23/02/2015

Research Institutions

Chatham House	Dave Clemente	London	07/05/2014
International Centre for Defence and Security	Piret Pernik	Tallinn	20/05/2014
Unaffiliated*	Lilli Traat, Susan Ristikivi		30/05/2014
Security and Defence Agenda	Pauline Massart	Brussels	16/06/2014

Academic Institutions

Tallinn University of Technology	Dr Rain Ottis	Tallinn (Skype)	26/06/2014
University of Warwick	Dr George Christou	Warwick (Skype)	18/09/2014

National Government Representations

UK Department of Business, Innovation and Skills		London	14/01/14, 16/05/14
UK Foreign and Commonwealth Office		London	08/05/2014
UK Cabinet Office		London	08/05/2014
Dutch National Cyber Security Centre		The Hague	23/05/2014
Representative of the Government of Estonia	Luukas Ilves	Brussels	12/06/2014
German Permanent Representative to the EU		Brussels	25/02/2015

*Permission to cite institute withheld

Appendix 11 – Control Codes (NVivo nodes) derived from EU Cyber Security Strategy

Code/Node Name	No. of Sources	No. of References
EUCSS Drivers - The EU is doing what it is doing because...	0	0
1. EU Values Offline also apply Online	12	19
1a. Protection of fundamental rights	79	157
2. The Internet needs to be robust and innovative	2	2
2a. To ensure freedom	1	2
2b. To ensure prosperity	1	1
3.a Private sector innovation must be encouraged	17	27
3.a.i. Through Private sector incentivisation	11	15
3b. Civil Society involvement must be encouraged	26	40
4a. The EU is seeking to protect cyberspace from incidents NIS	13	17
4b. The EU is seeking to protect cyberspace from Malicious Activities NIS	9	12
4c. The EU is seeking to protect cyberspace from Misuse NIS	2	4
4d. The EU is seeking to protect cyberspace from 4a-c because doing so is conducive to EU internal security NIS	4	5
4.d.i Internet's integrity and security must be guaranteed to allow safe access for all	7	8
5a. ECONOMIC Functioning of the Internal Market	70	169
5b. ECONOMIC Europe-wide market demand for secure products	4	5
5c. ECONOMIC Promote industry	23	27
5d. ECONOMIC Economic Growth	82	180
5e. ECONOMIC Reliance of economic sectors on ICT	16	21
5f. ECONOMIC Creating jobs	42	84
6. TRUST Build citizen trust in online transactions to boost commercial transactions and achieve economic potential	49	85

7. to protect the integrity of critical infrastructures (CIP) NIS	24	30
7a. Critical Information Infrastructure Protection NIS	25	29
8. Tackling cyber-crime CYBER-CRIME	70	116
8a. Protection of Children	38	65
9. Tackling international and state or government misuse of cyberspace	4	4
10. Keeping up with international political trends	4	6
11a. CORPORATE ACTOR European Commission	68	197
11b. CORPORATE ACTOR High Representative	2	3
11c. INSTITUTIONAL DRIVER Charter of Fundamental Rights of the EU	14	20
11d. INSTITUTIONAL DRIVER Budapest Convention	20	29
11e. INSTITUTIONAL DRIVER International Humanitarian Law	1	1
12. FACILITATION The EU is conducive to the internationality of cyberspace	41	70
12a. FACILITATION EU can manage multiple actors and actor types	33	68
12b. FACILITATION EU can facilitate Co-operation	111	380
12.b.i FACILITATION EU can facilitate co-operation between civil and military	7	9
12.b.ii FACILITATION EU can facilitate co-operation between EU Member States	36	64
12c. FACILITATION The EU is in a position to legislate	22	30
12d. FACILITATION EU facilitates raising awareness	45	77
13. Cyber defence CYBER DEFENCE	8	14
14....because of increased social, economic and political dependence on networked technologies	28	47
15. RESILIENCE	28	68
16. Member State responsibility	20	34
16a. Member States are the drivers INTERVIEWS	12	27

Appendix 12 – Codes (NVivo nodes) not derived from EUCSS

Code/Node Name	No. of Sources	No. of References
Non-EUCSS Drivers	0	0
NED 1. FRAGMENTATION	0	0
NED 1a. FRAGMENTATION of efforts between Member States	52	83
NED 1b. FRAGMENTATION of efforts between EU agencies	0	0
NED 1c. FRAGMENTATION of efforts between EU and MS	0	0
NED 1d. FRAGMENTATION of the market	11	12
NED 1e. FRAGMENTATION of EU approaches	7	8
NED 1f. FRAGMENTATION of networks	1	1
NED 2. INSTITUTIONAL DRIVERS	0	0
NED 2b. Digital Agenda for Europe	16	18
NED 2c INSTITUTIONAL DRIVER TEU and TFEU	2	4
NED 2d. INSTITUTIONAL DRIVER European Public Private Partnership for Resilience	2	2
NED 2f. INSTITUTIONAL DRIVER Lisbon Treaty	5	13
NED 2g. INSTITUTIONAL DRIVER Stockholm Programme	3	3
NED 2l. INSTITUTIONAL DRIVER Competences as defined in the Treaties INTERVIEWS	18	33
NED 3. CATALYIC DRIVERS	0	0
NED 3a. CATALYTIC Estonia 2007	14	21
NED 3b. CATALYTIC Conficker 2008	1	1
NED 3c. CATALYTIC 2008 Financial Crisis	2	3
NED 3d. CATALYTIC Lithuania	2	2
NED 3e. CATALYTIC Georgia 2008	5	5
NED 3f. CATALYTIC Establishment of Internal Market 1993	0	0
NED 3g. CATALYTIC September 11th	3	3

NED 3h. CATALYTIC Snowden	7	13
NED 3i. CATALYTIC 2011 Dutch child abuse case	1	1
NED 3j. CATALYTIC Sony Hack	1	1
NED 3k CATALYTIC London 7 July 2005 Bombings	1	1
NED 4. Information Society	21	50
NED 5. National Security	3	3
NED 6. Individual Impetus INTERVIEWS	22	61
NED 7. CORPORATE ACTORS	0	0
NED 7a. CORPORATE ACTOR Council of the European Union	28	43
NED 7b. CORPORATE ACTOR European Council	36	64
NED 7c. CORPORATE ACTOR European Forum for Member States	5	6
NED 7d. CORPORATE ACTOR EEAS INTERVIEWS	12	26
NED 7e. CORPORATE ACTOR European Parliament	16	20
NED 7f. CORPORATE ACTOR Friends of the Presidency INTERVIEWS	8	11
INTERVIEW DRIVERS	0	0
ID 1. EU is an economic institution	1	1
ID 2. Follow the money - look at where the EU is spending resource	4	5
ID 5. INSTITUTIONAL DRIVER Treaty of Lisbon	9	11
ID 7. Need for Coherence	7	9
ID 8. Reducing duplication of efforts	12	17

Appendix 13 – Article 222 TFEU: “Solidarity Clause”

SOLIDARITY CLAUSE Article 222 TFEU

1. The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:

(a) — prevent the terrorist threat in the territory of the Member States; — protect democratic institutions and the civilian population from any terrorist attack;

— assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;

(b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

2. Should a Member State be the object of a terrorist attack or the victim of a natural or manmade disaster, the other Member States shall assist it at the request of its political authorities. To that end, the Member States shall coordinate between themselves in the Council.

3. The arrangements for the implementation by the Union of the solidarity clause shall be defined by a decision adopted by the Council acting on a joint proposal by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy. The Council shall act in accordance with Article 31(1) of the Treaty on European Union where this decision has defence implications. The European Parliament shall be informed.

For the purposes of this paragraph and without prejudice to Article 240, the Council shall be assisted by the Political and Security Committee with the support of the structures developed in the context of the common security and defence policy and by the Committee referred to in Article 71; the two committees shall, if necessary, submit joint opinions.

4. The European Council shall regularly assess the threats facing the Union in order to enable the Union and its Member States to take effective action.

References

Acharya, V.V., Richardson, M., 2009. Causes of the Financial Crisis. Crit. Rev. 21, 195–210. doi:10.1080/08913810902952903

Alexander, G., 2001. Institutions, path dependence, and democratic consolidation. J. Theor. Polit. 13, 249–269.

Antezana, M.E., 2003. European Union Internet Copyright Directive as Even More Than It Envisions: Toward a Supraeu Harmonization of Copyright Policy and Theory, The. BC Intl Comp Rev 26, 415.

Arquilla, J., Ronfeldt, D., 1993. Cyberwar is coming! Comp. Strategy 12, 141–165. doi:10.1080/01495939308402915

Baba, N., Packer, F., 2009. From turmoil to crisis: dislocations in the FX swap market before and after the failure of Lehman Brothers. J. Int. Money Finance 28, 1350–1374.

Bache, I., George, S., Bulmer, S., 2011. Politics in the European Union. OUP.

Bangemann, M., 1994. Recommendations to the European Council: Europe and the global information society.

Bannerman, S., Haggart, B., 2014. Historical Institutionalism in Communication Studies. Commun. Theory n/a-n/a. doi:10.1111/comt.12051

Baumgartner, F.R., Jones, B.D., Mortensen, P.B., 2014. Punctuated equilibrium theory: Explaining stability and change in public policymaking, in: Sabatier, P.A., Weible, C.M. (Eds.), Theories of the Policy Process. pp. 59–103.

Bendiek, A., 2012. European cyber security policy. SWP Res. Pap. 13.

Bendiek, A., Porter, A.L., 2013. European Cyber Security Policy within a Global Multistakeholder Structure. Eur. Foreign Aff. Rev. 18, 155–180.

Bennett, A., 2010. Process Tracing and Causal Inference, in: Brady, H.E., Collier, D. (Eds.), Rethinking Social Inquiry: Diverse Tools, Shared Standards. Rowman & Littlefield Publishers, pp. 207–219.

Bennett, A., Checkel, J.T. (Eds.), 2015. Process tracing: from metaphor to analytic tool, Strategies for social inquiry. Cambridge University Press, Cambridge.

Bennett, S.C., 2012. Right to Be Forgotten: Reconciling EU and US Perspectives, The. Berkeley J. Int. Law 30, 161.

Berg, B.L., 2004. Qualitative research methods for the social sciences, 5th ed., international student ed. ed. Pearson, Boston, Mass. ; London.

Biernacki, P., Waldorf, D., 1981. Snowball sampling: Problems and techniques of chain referral sampling. Sociol. Methods Res. 10, 141–163.

Blundell, C., Raghavan, A., Martin, M.M., 2010. RETCON: transactional repair without replay, in: ACM SIGARCH Computer Architecture News. ACM, pp. 258–269.

Blythe, S.E., 2008. Croatia's computer laws: promotion of growth in E-commerce via greater cyber-security. Eur. J. Law Econ. 26, 75–103.

Boin, A., Busuioc, M., Groenleer, M., 2014. Building European Union capacity to manage transboundary crises: Network or lead-agency model? Regul. Gov. 8, 418–436.

Bossong, R., 2014. The European Programme for the protection of critical infrastructures – meta-governing a new security problem? Eur. Secur. 0, 1–17. doi:10.1080/09662839.2013.856307

Bretherton, C., Vogler, J., 2006. The European Union as a global actor. Routledge.

Briglauer, W., 2014. The impact of regulation and competition on the adoption of fiber-based broadband services: recent evidence from the European union member states. J. Regul. Econ. 46, 51–79.
Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., Chon, S., 2014. An Analysis of the Nature of Groups Engaged in Cyber Crime. Int. J. Cyber Criminol. 8, 1–20.
Bryman, A., 2008. Social research methods, 3rd ed. ed. Oxford University Press, Oxford.
Bucci, S., 2012. Joining Cybercrime and Cyberterrorism: A Likely Scenario, in: Reveron, D.S. (Ed.), Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Georgetown University Press, pp. 57–70.
Bucher, R., Fritz, C.E., Quarantelli, E.L., 1956. Tape Recorded Interviews in Social Research. Am. Sociol. Rev. 21, 359–364. doi:10.2307/2089294
Bulmer, S., 2009. Politics in time meets the politics of time: historical institutionalism and the EU timescape. J. Eur. Public Policy 16, 307–324.
Bulmer, S., 2008. Theorizing Europeanization, in: Graziano, P., Vink, M.P. (Eds.), Europeanization. Palgrave Macmillan UK, pp. 46–58.
Bulmer, S., 1998. New institutionalism and the governance of the Single European Market. J. Eur. Public Policy 5, 365–386.
Bulmer, S., 1997. New institutionalism, the Single Market and EU governance.
Bulmer, S., Burch, M., 2001. The "Europeanisation" of central government: the UK and Germany in historical institutionalist perspective. Rules Integr. Institutionalist Approaches Study Eur. 73–96.
Bulmer, S., Padgett, S., 2005. Policy transfer in the European Union: an institutionalist perspective. Br. J. Polit. Sci. 35, 103–126.
Burnham, P., Lutz, K.G., Grant, W., Layton-Henry, Z., 2008. Research methods in politics. Palgrave Macmillan.
Cafruny, A.W., Ryner, M., 2003. A ruined fortress?: neoliberal hegemony and transformation in Europe. Rowman & Littlefield.
Carmassi, J., Gros, D., Micossi, S., 2009. The Global Financial Crisis: Causes and Cures*. JCMS J. Common Mark. Stud. 47, 977–996. doi:10.1111/j.1468-5965.2009.02031.x
Carrapiço, H., Trauner, F., 2013. Europol and its influence on EU policy-making on organized crime: analyzing governance dynamics and opportunities. Perspect. Eur. Polit. Soc. 14, 357–371.
Centeno, C., Van Bavel, R., Burgelman, J.-C., 2005. A prospective view of e-government in the European Union. Electron. J. E-Gov. 3, 59–66.
Checkel, J.T., 1999. Social construction and integration. J. Eur. Public Policy 6, 545–560. doi:10.1080/135017699343469
Checkel, J.T., Moravcsik, A., 2001. A constructivist research program in EU studies? Eur. Union Polit. 2, 219–249.
Choucri, N., Madnick, S., Ferwerda, J., 2014. Institutions for Cyber Security: International Responses and Global Imperatives. Inf. Technol. Dev. 20, 96–121. doi:10.1080/02681102.2013.836699
Christiansen, T., Dobbels, M., 2013. Delegated Powers and Inter-Institutional Relations in the EU after Lisbon: A Normative Assessment. West Eur. Polit. 36, 1159–1177. doi:10.1080/01402382.2013.826023

Christou, G., 2016. Cyber Security in the European Union: Resilience and Adaptability in an Age of Governance, New Security Challenges. Palgrave Macmillan, Houndmills, Basingstoke.

Christou, G., Simpson, S., 2014. Shaping the global communications milieu: The EU's influence on Internet and telecommunications governance. Comp. Eur. Polit. 12, 54–75. doi:10.1057/cep.2012.33

Clandinin, D.J., Connelly, F.M., others, 2000. Narrative inquiry: Experience and story in qualitative research.

Coffee Jr, J.C., 2009. What went wrong? An initial inquiry into the causes of the 2008 financial crisis. J. Corp. Law Stud. 9, 1–22.

Collier, R.B., Collier, D., 1991. Critical Junctures and Historical Legacies.

Conway, M., 2005. Cybercortical Warfare: Hizbollah's Internet Strategy, in: Oates, S., Owen, D., Gibson, R. (Eds.), The Internet and Politics; Citizens, Voters and Activists. Routledge.

Cornish, P., 2009. Cyber Security and Politically, Socially and Religiously motivated Cyber Attacks (Study), Directorate General External Policies of the Union. European Parliament.

Council of Europe, 2001. Convention on Cybercrime.

Council of The European Union, 2013a. Council Conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy joint communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (June 2013).

Council of The European Union, 2013b. Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace July 2013.

Council of The European Union, 2013c. Council Decision of 3 December 2013 establishing the specific programme implementing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decisions 2006/971/EC, 2006/972/EC, 2006/973/EC, 2006/974/EC and 2006/975/EC (Text with EEA relevance) (2013/743/EU), (2013/743/EU).

Council of The European Union, 2012. Declaration on the Launch of the Global Alliance against child sexual abuse online.

Council of The European Union, 2011a. Draft Council Conclusions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" (CIIP) - Presidency text.

Council of The European Union, 2011b. PREPARATION OF THE TTE COUNCIL MEETING (TRANSPORT, TELECOMMUNICATIONS, ENERGY) ON 27 MAY 2011 Draft Council Conclusions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" (CIIP) 10003/11.

Council of The European Union, 2011c. Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" (CIIP) - Adoption of Council conclusions 10299/11.

Council of The European Union, 2011d. Council conclusions on the protection of children in the digital world.

Council of The European Union, 2009. Position of the Netherlands on fighting cyber-crime.

Council of The European Union, 2008. Comprehensive Plan to Combat Cyber Crime 11784/08.
Council of The European Union, 2007. Council Conclusions.
Council of The European Union, 2003. Note from the Presidency to the Council: Stimulating the European digital content: legislation and policies - Exchange of views.
Council of The European Union, 2002a. Draft Council Resolution on "Preserving tomorrow's memory - preserving digital content for future generations."
Council of The European Union, 2002b. Introductory Note from the Permanent Representatives Committe to the Council: Draft Council Resolution on "Preserving tomorrow's memory - preserving digital content for future generations."
Council of The European Union, 2002c. Outcome of Proceedings of Working Party on Telecommunications.
Council of The European Union, 1997. Resolution of the Council and of the Representatives of the Governments of the Member States, meeting within the Council of 17 February 1997 on illegal and harmful content on the Internet (97 /C 70/01).
Council of the European Union, 1991. Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs.
Council of The European Union, Friends of the Presidency on Cyber Issues, 2012. NOTICE OF MEETING AND PROVISIONAL AGENDA.
Crago, P.G., 1996. Fundamental Rights on the Infobahn: Regulating the Delivery of Internet Related Services Within the European Union. Hastings Intl Comp Rev 20, 467.
Craig, P., 2010. The Lisbon Treaty: law, politics, and treaty reform. OUP.
Craig, P., 2008. The Treaty of Lisbon: Process, architecture and substance. Eur. Law Rev. 137–166.
Cram, L., 1996. Integration theory and the study of the European policy process, in: Richardson, J. (Ed.), European Union: Power and Policy-Making. Routledge, London, pp. 40–58.
Cresswell, J.W., 1998. Qualitative inquiry and research design: Choosing among five traditions. Sage Publications.
Crotty, J., 2009. Structural causes of the global financial crisis: a critical assessment of the "new financial architecture." Camb. J. Econ. 33, 563–580. doi:10.1093/cje/bep023
De Werra, J., 2002. The legal system of technological protection measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union directives and other national laws (Japan, Australia).
Deibert, R.J., 2009. The geopolitics of internet control: Censorship, sovereignty, and cyberspace, in: Chadwick, A., Howard, P.N. (Eds.), Routledge Handbook of Internet Politics. Routledge, London, pp. 323–336.
Dewar, R., 2014. The "Triptych of Cyber Security": A Classification of Active Cyber Defence, in: Prangetto, P., Maybaum, M., Stinissen, J. (Eds.), 6th International Conference on Cyber Conflict. NATO CCD COE Publications, pp. 7–22.
Dewar, R., 2012. The Role of the European Union in Providing and Ensuring Cybersecurity in Europe (Masters Degree Dissertation). University of Glasgow, Glasgow.

Dinan, D., 2010. Ever closer union: an introduction to European integration, 4th ed. Rienner, Boulder, Colorado.
Dinstein, Y., 2012. The Principle of Distinction and Cyber War in International Armed Conflicts. J. Confl. Secur. Law 17, 261–277. doi:10.1093/jcsl/krs015
Duke, S., 2011. Pax or Pox Europeana after the Lisbon Treaty? Int. Spect. 46, 83–99. doi:10.1080/03932729.2011.549756
Dunn Cavelty, M., 2013. A resilient Europe for an open, safe and secure cyberspace. UI Occassional Pap. 23.
Dunn Cavelty, M., 2012a. Cyber-security, in: Collins, A. (Ed.), Contemporary Security Studies. OUP.
Dunn Cavelty, M., 2012b. The Militarisation of Cyber Security as a Source of Global Tension, in: Möckli, D., Wenger, A. (Eds.), Strategic Trends Analysis. Center for Security Studies, Zurich, Switzerland.
EEAS, n.d. EEAS - About CSDP: The Petersberg Tasks [WWW Document]. URL http://www.eeas.europa.eu/csdp/about-csdp/petersberg/index_en.htm
ENISA, 2013. National Cyber Security Strategies in the World — ENISA [WWW Document]. URL http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (accessed 2.8.13).
ENISA, 2012. Cyber Europe 2012 - Key Findings Report. ENISA.
ENISA, 2011a. Technical Guideline on Minimum Security Measures — ENISA [WWW Document]. URL http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/minimum-security-requirements/copy_of_minimum-security-requirements/technical-guideline-on-minimum-security-measures (accessed 8.17.13).
ENISA, 2011b. Cyber Europe 2010 Report — ENISA [WWW Document]. URL http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report (accessed 8.6.12).
ENISA, 2011c. Cyber Atlantic — ENISA [WWW Document]. URL http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic (accessed 8.18.13).
ENISA, 2005. Activities — ENISA [WWW Document]. URL http://www.enisa.europa.eu/about-enisa/activities (accessed 8.12.13).
EPP, n.d. Who are we? [WWW Document]. Who Are We. URL http://www.epp.eu/who-are-we
Estonia, 2008. Cyber Security Strategy (National Strategy). Cyber Security Strategy Committee, Ministry of Defence, Tallinn, Estonia.
Etherington, K., 2013. Narrative approaches to case studies. Last Accessed 30.
Eurojust, n.d. History of Eurojust [WWW Document]. URL http://www.eurojust.europa.eu/about/background/Pages/history.aspx (accessed 3.20.16).
Europa, n.d. EUROPA - EU treaties [WWW Document]. URL http://europa.eu/eu-law/decision-making/treaties/index_en.htm (accessed 12.21.15).
European Commission, 2016a. European Commission - PRESS RELEASES - Press release - Statement by Vice-President Ansip and Commissioner Oettinger welcoming the adoption of the first EU-wide rules on cybersecurity [WWW Document]. URL http://europa.eu/rapid/press-release_STATEMENT-16-2424_en.htm (accessed 10.23.16).
European Commission, 2016b. The Directive on security of network and information systems (NIS Directive) [WWW Document]. Digit. Single Mark. URL

https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (accessed 9.26.16).

European Commission, 2013a. JOIN (2013) 1 Final Joint Communication to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (Communication). European Commission.

European Commission, 2013b. COM (2013) 48 final 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.

European Commission, 2012a. Cyber Security in Europe: European Policy and Legislative Documents relevant for Cybersecurity.

European Commission, 2012b. COM (2012) 0140 Final Communication from the Commission to the Council and the European Parliament - Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre.

European Commission, 2012c. COM (2012) 196 final European Strategy for a Better Internet for Children.

European Commission, 2011a. COM (2011) 163 Final Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Achievements and next steps: towards global cyber-security" (Communication).

European Commission, 2011b. COM (2011) 60 Final Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions - An EU Agenda for the Rights of the Child (Communication).

European Commission, 2011c. COM (2011) 566 final Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the application of the Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity and of the Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and online information services industry -PROTECTING CHILDREN IN THE DIGITAL WORLD (Report/Study).

European Commission, 2010a. COM(2010) 517 final Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (Communication). European Commission.

European Commission, 2010b. SEC (2010) 1123 final COMMISSION STAFF WORKING DOCUMENT SUMMARY OF THE IMPACT ASSESSMENT Accompanying document to the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on attacks against information systems, and repealing Council Framework Decision 2005/222/JHA (Communication). European Commission.

European Commission, 2010c. COM (2010) 245 Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions - A Digital Agenda for Europe (Communication). European Commission.

European Commission, 2010d. COM (2010) 608 final/2 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Towards a Single Market Act For a highly competitive social market economy 50 proposals for improving our work, business and exchanges with one another.

European Commission, 2010e. COM (2010) 521 final Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Concerning the European Network and Information Security Agency (ENISA) (Communication). European Commission.

European Commission, 2010f. COM (2010) 171 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the - Delivering an area of freedom, security and justice for Europe's citizens Action Plan Implementing the Stockholm Programme (Communication). European Commission.

European Commission, 2010g. COM (2010) 673 Final Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (Communication). European Commission.

European Commission, 2009a. COM (2009) 149 Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions - Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.

European Commission, 2009b. COM (2009) 324 final Modernising ICT Standardisation in the EU - The Way Forward.

European Commission, 2007a. COM (2007) 267 final Communication from the Commission to the European Parliament, The Council and the Committee of the Regions - Towards a general policy the fight against cyber crime.

European Commission, 2007b. SEC (2007) 641 Commission Staff Working Document - Accompanying document to the Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the Fight against Cyber crime - Summary of the Impact Assessment (Working Document). European Commission.

European Commission, 2006a. COM (2006) 251 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - A Strategy for a Secure Information Society – "Dialogue, partnership and empowerment."

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

European Commission, 2005. COM (2005) 229 Final Communication from the Commission to the Council, the European Parliament, The European Economic and Social Committee and the Committee of the Regions - "i2010 – A European Information Society for growth and employment."

European Commission, 2001a. COM (2001) 298 Final 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 (Communication). European Commission.

European Commission, 2001b. COM (2001) 140 Commission Report to Euco eEurope 2002 Impact and Priorities (Communication). European Commission.

European Commission, 2000a. COM (2000) 130 Commission report: eEurope — an Information Society for All; progress report for the Special European Council on Employment, Economic Reforms and Social Cohesion: Towards a Europe based on Innovation and Knowledge. [WWW Document]. URL http://www.publications.parliament.uk/pa/cm199900/cmselect/cmeuleg/23-xvi/2314.htm (accessed 8.20.13).

European Commission, 2000b. COM (2000) 890 Final Communication from the Commission to the Council, the European Parliament, The European Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime [WWW Document]. URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:html (accessed 8.20.13).

European Commission, 1999. eEurope - An information society for all [WWW Document]. URL http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l24221 (accessed 1.22.16).

European Commission, 1998. COM (1998) 50 final Globalisation and the Information Society: The Need for Strengthened International Co-ordination [WWW Document]. URL (accessed 8.20.13).

European Commission, 1997a. COM (97) 157 European Initiative on Electronic Commerce [WWW Document]. URL http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51997DC0157&from=EN

European Commission, 1997b. COM (97) 582 Final Action Plan on Promoting Safe Use of the Internet [WWW Document].

European Commission, 1997c. COM (97) 503 Ensuring Security and Trust in Electronic Communications: Towards a European Framework for Digital Signatures and Encryption.

European Commission, 1996a. COM (96) 487 Illegal and Harmful Content on the Internet.

European Commission, 1996b. COM (96) 389 Final Green Paper on Living and Working in the Information Society: People First.

European Commission, 1996c. COM (96) 395 The Information Society: From Corfu to Dublin The new emerging priorities.

European Commission, 1996d. COM (96) 471 LEARNING IN THE INFORMATION SOCIETY Action plan for a European education initiative (1996-98).

European Commission, 1996e. COM (96) 607 Europe at the Forefront of the Global Information Society: Rolling Action Plan.

European Commission, 1996f. COM (96) 483 Green Paper on the protection of minors and human dignity in audiovisual and info services.

European Commission, 1995. COM (95) 492 Final Report from the Commission to the Council, the Euoprean Parliament and the Economic and Social Committee on the main events and developments in the information market 1993-1994 [WWW Document]. URL http://aei.pitt.edu/5857/1/5857.pdf

European Commission, 1994. COM (94) 347 Final Europe's Way to the Information Society: An Action Plan [WWW Document].

European Commission, 1993. COM (93) 700 White Paper - Growth, Competitiveness and Employment: The Challenges and Ways forward into the 21st Century [WWW Document].

European Commission, 1992a. COM (92) 24 Final Commission Proposal for a Council Directive on the legal protection of databases [WWW Document].

European Commission, 1992b. COM (92) 422 Final Commission proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data [WWW Document]. URL http://aei.pitt.edu/10375/1/10375.pdf (accessed 2.25.14).

European Commission, 1985. COM (85) 310 final Completing the Internal Market: White Paper from the Commission to the European Council (White Paper No. COM (85) 310 final). European Commission, Brussels.

European Council, 2014. The President of the European Council [WWW Document]. URL http://www.consilium.europa.eu/en/european-council/president/ (accessed 1.19.15).

European Council, 2011a. European Council Conclusions 2011 December.

European Council, 2011b. European Council Conclusions 2011 October.

European Council, 2010. European Council Conclusions 2010 June.

European Council, 2008. European Council Conclusions 2008 December Brussels.

European Council, 2003a. European Council Conclusions 2003 March Brussels.

European Council, 2003b. European Council Conclusions 2003 October Brussels.

European Council, 2002. European Council Conclusions 2002 March Barcelona.

European Council, 2001. European Council Conclusions 2001 March Stockholm.

European Council, 1994a. European Council Conclusions 1994 December Essen.

European Council, 1994b. European Council Conclusions 1994 June Corfu.

European Council, 1993a. European Council Conclusions 1993 June Copenhagen.

European Council, 1993b. European Council Conclusions 1993 December Brussels.

European Council, 1992. European Council Conclusions 1992 December Edinburgh.

European Council, Council of the European Union, 2014. The European Council and the Council of the European Union [WWW Document]. URL http://www.consilium.europa.eu/en/home/ (accessed 1.19.15).

European Parliament, n.d. Organisation and Work of the Euoropean Parliament [WWW Document]. URL http://www.europarl.europa.eu/aboutparliament/en/0025729351/Organisation-and-work.html (accessed 1.19.15).

European Parliament, Council of The European Union, 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union.

European Parliament, Council of The European Union, 2013a. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

European Parliament, Council of The European Union, 2013b. Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.

European Parliament, Council of The European Union, 2012. Regulation (EU) No 1024/2012 Of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ("the IMI Regulation").

European Parliament, Council of The European Union, 2011. Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework- Decision 2004/68/JHA.

European Parliament, Council of the European Union, 2009. Directive 2009/140/EC of the European Parliament and of the Council.

European Parliament, Council of the European Union, 2008. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

European Parliament, Council of The European Union, 2004. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance).

European Parliament, Council of The European Union, 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [WWW Document]. Off. J. 201 31072002 P 0037 - 0047. URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (accessed 8.20.13).

European Parliament, Council of the European Union, 2002a. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

European Parliament, Council of the European Union, 2002b. Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).

European Parliament, Council of The European Union, 1997. DIRECTIVE 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

European Parliament, Council of The European Union, 1996. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

European Parliament, Council of The European Union, 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

European Union, 2016. EUROPA - Foreign and Security Policy [WWW Document]. Eur. Union Website Off. EU Website - Eur. Comm. URL https://europa.eu/european-union/topics/foreign-security-policy_en (accessed 10.23.16).
European Union, 2009a. Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. Off. J.
European Union, 2009b. Treaty on the Functioning of the European Union.
European Union, 2007. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community.
European Union, 1995. Subsidiarity [WWW Document]. URL http://europa.eu/legislation_summaries/glossary/subsidiarity_en.htm (accessed 8.15.12).
European Union, 1992. Treaty of Maastricht on European Union.
European Union, 1987. Single European Act.
European Union, n.d. Community acquis [WWW Document]. URL http://eur-lex.europa.eu/summary/glossary/acquis.html (accessed 8.15.12a).
European Union, n.d. Division of competences within the European Union [WWW Document]. URL http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:ai0020&from=EN (accessed 10.16.16b).
European Union, n.d. EUROPA - Regulations, Directives and other acts [WWW Document]. URL http://europa.eu/about-eu/basic-information/decision-making/legal-acts/index_en.htm (accessed 8.11.12c).
Europol, 2013a. A Collective EU Response to Cybercrime [WWW Document]. URL https://www.europol.europa.eu/ec3 (accessed 2.1.13).
Europol, 2013b. History: The First Years 1992-2004 [WWW Document]. URL https://www.europol.europa.eu/content/page/first-years
Europol, 2013c. History [WWW Document]. URL https://www.europol.europa.eu/content/page/history-149
Europol, 2013d. Mandate [WWW Document]. URL https://www.europol.europa.eu/content/page/mandate-119
Europol, n.d. Combating Cybercrime in a Digital Age [WWW Document]. URL https://www.europol.europa.eu/ec3/ (accessed 10.23.16).
Falessi, N., Gavrila, R., Klejnstrup, M.R., Moulinos, K., 2012. National Cyber Security Strategies: An Implementation Guide — ENISA [WWW Document]. URL http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide (accessed 8.17.13).
Farwell, J.P., Rohozinski, R., 2011. Stuxnet and the future of cyber war. Survival 53, 23–40.
Faugier, J., Sargeant, M., 1997. Sampling hard to reach populations. J. Adv. Nurs. 26, 790–797.
Fidler, D.P., 2012. Inter arma silent leges Redux? The Law of Armed Conflict and Cyber Conflict, in: Reveron, D.S. (Ed.), Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Georgetown University Press, pp. 71–88.
Fligstein, N., Mara-Drita, I., 1996. How to make a market: reflections on the attempt to create a single market in the European Union. Am. J. Sociol. 1–33.
Follesdal, A., 2013. Competing conceptions of subsidiarity.

Gasper, D., Apthorpe, R., 1996. Introduction: Discourse analysis and policy discourse. Eur. J. Dev. Res. 8, 1–15. doi:10.1080/09578819608426650
Gaycken, S., 2012. Cyberwar-Das Wettrüsten hat längst begonnen: Vom digitalen Angriff zum realen Ausnahmezustand. Goldmann Verlag.
Gaycken, S., 2011. Cyberwar: Das Internet als Kriegsschauplatz. Open Source Press, Munich, Germany.
George, A.L., Bennett, A., 2005. Case studies and theory development in the social sciences. Mit Press.
Gibson, W., 1984. Neuromancer. Victor Gollancz, London.
Gleick, J., 1997. Chaos: Making a new science. Random House.
Goldstone, J.A., 1991. Revolution and rebellion in the early modern world. Univ of California Press.
Golub, J., 1996. Sovereignty and Subsidiarity in EU Environmental Policy. Polit. Stud. 44, 686–703. doi:10.1111/j.1467-9248.1996.tb01749.x
Goodman, J.W., 2006. Telecommunications Policy-making in the European Union. Edward Elgar Publishing.
Greenwald, G., MacAskill, E., 2013. Boundless Informant: the NSA's secret tool to track global surveillance data. The Guardian.
Haas, E.B., 1970. The study of regional integration: reflections on the joy and anguish of pretheorizing. Int. Organ. 24, 607–646.
Haas, E.B., 1961. International integration: the European and the universal process. Int. Organ. 15, 366–392.
Haas, E.B., 1958. The uniting of Europe. University of Notre Dame Press Notre Dame, IN.
Hall, P.A., 1992. The movement from Keynesianism to monetarism: Institutional analysis and British economic policy in the 1970s, in: Steinmo, S., Thelen, K.A., Longstreth, F. (Eds.), Structuring Politics: Historical Institutionalism in Comparative Analysis, Cambridge Studies in Comparative Politics. Cambridge University Press, Cambridge, pp. 90–113.
Hall, P.A., Franzese, R.J., others, 1998. Mixed signals: central bank independence, coordinated wage bargaining, and European Monetary Union. Int. Organ. 52, 505–535.
Hall, P.A., Taylor, R.C.R., 1996. Political Science and the Three New Institutionalisms*. Polit. Stud. 44, 936–957.
Handmer, J.W., Dovers, S.R., 1996. A Typology of Resilience: Rethinking Institutions for Sustainable Development. Organ. Environ. 9, 482–511. doi:10.1177/108602669600900403
Hansen, L., Nissenbaum, H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. Int. Stud. Q. 53, 1155–1175. doi:10.1111/j.1468-2478.2009.00572.x
Hardaker, C., 2010. Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. J. Politeness Res. 6, 215–242.
Healey, J. (Ed.), 2013. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Atlantic Council, CCSA.
Herring, S., Job-Sluder, K., Scheckler, R., Barab, S., 2002. Searching for safety online: Managing" trolling" in a feminist forum. Inf. Soc. 18, 371–384.
Herzog, M., Prior, T., 2013. The Practical Application of Resilience: Resilience Manifestation and Expression. Eidgenössische Technische Hochschule (Zürich) Risk and Resilience Research Group Schweiz Bundesamt für Bevölkerungsschutz.

Hoffmann, S., 1966. Obstinate or obsolete? The fate of the nation-state and the case of Western Europe. Daedalus 862–915.
Howorth, J., 2013. European security institutions 1945-2010: the weaknesses and strengths of "Brusselsization," in: Biscop, S., Whitman, R.G. (Eds.), The Routledge Handbook of European Security. pp. 5–17.
Huntington, S.P., 1968. Political order in changing societies. Yale University Press.
Hycner, R.H., 1985. Some guidelines for the phenomenological analysis of interview data. Hum. Stud. 8, 279–303.
Hyde-Price, A., Jeffery, C., 2001. Germany in the European Union: Constructing Normality. JCMS J. Common Mark. Stud. 39, 689–717. doi:10.1111/1468-5965.00327
Interview, Clemente, Chatham House, D., 2014. Interview - Cyber Security and the European Union (PhD) (PwC).
Interview, de Vries, National Cyber Security Centre of the Netherlands, P., 2014. Interview - Cyber Security and the European Union (PhD) (NCSC).
Interview, Helmbrecht, ENISA, P.D.U., 2014. Interview - Cyber Security and the European Union (PhD) (ENISA).
Interview, Ilves, Govt. of Estonia, L., 2014. Interview - Cyber Security and the European Union (PhD) (Govt. of Estonia).
Interview, Massart, SDA, P., 2014. Interview - Cyber Security and the European Union (PhD) (SDA).
Interview, Ottis, Tallinn University of Technology, R., 2014. Interview - Cyber Security and the European Union (PhD).
Interview, Permanent Representation of Germany to the EU, 2015. Interview - Cyber Security and the European Union (PhD) (PermRep Germany).
Interview, Pernik, ICDS, P., 2014. Interview - Cyber Security and the European Union (PhD) (ICDS).
Interview, Purser, ENISA, D.S., 2014. Interview - Cyber Security and the European Union (PhD) (ENISA).
Interview, Roehrig, EDA, W., 2014. Interview - Cyber Security and the European Union (PhD) (EDA).
Interview, Rönnlund, DG Connect, A.-S., 2015. Interview - Cyber Security and the European Union (PhD) (DG Connect).
Interview, Senior Official, BEPA, European Commission, 2014. Interview - Cyber Security and the European Union (PhD) (BEPA).
Interview, Senior Official, BIS UK, 2014. Interview - Cyber Security and the European Union (PhD) (BIS, May).
Interview, Senior Official, CERT-EU, 2014. Interview - Cyber Security and the European Union (PhD) (CERT-EU).
Interview, Senior Official, DG Connect, European Commission, 2014. Interview - Cyber Security and the European Union (PhD) (DG Connect).
Interview, Senior Official, DG HOME, European Commission, 2014. Interview - Cyber Security and the European Union (PhD) (DG HOME).
Interview, Senior Official, DG MARKT, European Commission, 2014. Interview - Cyber Security and the European Union (PhD) (DG MARKT).
Interview, Senior Official, EC3, 2014. Interview - Cyber Security and the European Union (PhD) (EC3).
Interview, Senior Official, EEAS, 2014. Interview - Cyber Security and the European Union (PhD) (EEAS).

Interview, Senior Official, European Union, 2014. Interview - Cyber Security and the European Union (PhD).
Interview, Senior Official, Europol, 2014. Interview - Cyber Security and the European Union (PhD) (Europol).
Interview, Senior Official, UK Cabinet Office, 2014. Interview - Cyber Security and the European Union (PhD) (UK Cabinet Office).
Interview, Senior Official, UK Foreign and Commonwealth Office, 2014. Interview - Cyber Security and the European Union (PhD) (UK FCO).
Interview, Smith and Jones, eu-LISA, J., 2014. Interview - Cyber Security and the European Union (PhD) (eu-LISA).
Interview, Traat, L., Ristikivi, S., 2014. Interview - Cyber Security and the European Union (PhD).
Janczewski, L., Colarik, A.M., 2007. Cyber warfare and cyber terrorism. IGI Global.
Japan, 2013. Cyber Security Strategy of Japan.
Josselson, R., Lieblich, A., 2003. A framework for narrative research proposals in psychology., in: Josselson, R., Lieblich, A., McAdams, D.P. (Eds.), Up Close and Personal: The Teaching and Learning of Narrative Research. American Psychological Association.
Jupille, J., Caporaso, J.A., 1999. INSTITUTIONALISM AND THE EUROPEAN UNION: Beyond International Relations and Comparative Politics. Annu. Rev. Polit. Sci. 2, 429–444. doi:10.1146/annurev.polisci.2.1.429
Kabanov, Y., 2013. Information (Cyber-) Security Discourses and Policies in the European Union and Russia: A Comparative Analysis. Foresight.
Kaunert, C., Zwolski, K., 2014. Somalia versus Captain “Hook”: assessing the EU’s security actorness in countering piracy off the Horn of Africa. Camb. Rev. Int. Aff. 27, 593–612.
Kern, S., 2016. European Leaders Discuss Plan for European Army [WWW Document]. Gatestone Inst. URL https://www.gatestoneinstitute.org/8935/european-army (accessed 10.29.16).
Kerremans, B., 1996. Do Institutions Make a Difference? Non-Institutionalism, Neo-Institutionalism, and the Logic of Common Decision-Making in the European Union. Governance 9, 217–240. doi:10.1111/j.1468-0491.1996.tb00239.x
Kersbergen, K.V., Verbeek, B., 2007. The Politics of International Norms: Subsidiarity and the Imperfect Competence Regime of the European Union. Eur. J. Int. Relat. 13, 217–238. doi:10.1177/1354066107076955
King, G., Keohane, R.O., Verba, S., 1994. Designing social inquiry: Scientific inference in qualitative research. Princeton University Press.
Klimburg, A., Tiirmaa-Klaar, H., 2011. Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU. European Parliament.
Knill, C., Lenschow, A., 1998. Coping with Europe: the impact of British and German administrations on the implementation of EU environmental policy. J. Eur. Public Policy 5, 595–614. doi:10.1080/13501769880000041
Kornelius, S., 2016. Vor Gipfeltreffen: Deutschland und Frankreich wollen Verteidigungspolitik der EU reformieren. sueddeutsche.de.
Koslowski, R., 1999. A constructivist approach to understanding the European Union as a federal polity. J. Eur. Public Policy 6, 561–578. doi:10.1080/135017699343478

Kovats, L., 2009. Do elections set the pace? A quantitative assessment of the timing of European legislation. J. Eur. Public Policy 16, 239–255. doi:10.1080/13501760802589255
Krasner, S.D., 1984. Approaches to the State: Alternative Conceptions and Historical Dynamics. Comp. Polit. 16, 223–246. doi:10.2307/421608
Kruger, D., 2012. Radically Simplifying Cybersecurity.
Lachow, I., 2013. Active Cyber Defense: A Framework for Policymakers (Policy Brief). Center for North American Security, Washington, DC.
Lester, S., 1999. An introduction to phenomenological research.
Liberatore, A., 2007. Balancing security and democracy, and the role of expertise: Biometrics politics in the European Union. Eur. J. Crim. Policy Res. 13, 109–137.
Lindner, J., Rittberger, B., 2003. The Creation, Interpretation and Contestation of Institutions — Revisiting Historical Institutionalism. JCMS J. Common Mark. Stud. 41, 445–473. doi:10.1111/1468-5965.00430
Lindsay, J.R., 2013. Stuxnet and the Limits of Cyber Warfare. Secur. Stud. 22, 365–404. doi:10.1080/09636412.2013.816122
Lischka, K., 2013. Angriffe auf US-Firmen: Hacker hatten Zugang zu US-Pipeline-Steuerung. Spieg. Online.
Locher, B., 2012. Gendering the EU Policy Process and Constructing the Gender Acquis, in: Abels, G., Mushaben, J.M. (Eds.), Gendering the European Union, Gender and Politics Series. Palgrave Macmillan UK, pp. 63–84.
Mahoney, J., 2000. Path dependence in historical sociology. Theory Soc. 29, 507–548.
Manners, I., 2007. Another Europe is possible: critical perspectives on European Union politics. Handb. Eur. Union Polit. 77–95.
March, J.G., Olsen, J.P., 1989. Rediscovering Institutions. Simon and Schuster.
Martin, G., 2014. Notes on Willing Suspension of Disbelief. Retrieved.
McGraw, G., 2013. Cyber War is Inevitable (Unless We Build Security In). J. Strateg. Stud. 36, 109–119. doi:10.1080/01402390.2012.742013
Melvin, M., Taylor, M.P., 2009. The global financial crisis: Causes, threats and opportunities. Introduction and overview. J. Int. Money Finance, The Global Financial Crisis: Causes, Threats and Opportunities 28, 1243–1245. doi:10.1016/j.jimonfin.2009.08.002
Mendez, F., 2005. The European Union and cybercrime: insights from comparative federalism. J. Eur. Public Policy 12, 509–527. doi:10.1080/13501760500091737
Meyer, T., 2012. Graduated response in france: The clash of copyright and the internet. J. Inf. Policy 2, 107–127.
Meyer-Sahling, J.-H., Goetz, K.H., 2009. The EU timescape: from notion to research agenda. J. Eur. Public Policy 16, 325–336. doi:10.1080/13501760802589404
Moravcsik, A., 1993. Preferences and power in the European Community: a liberal intergovernmentalist approach. J. Common Mark. Stud. 31, 473–473.
Morris, T., Vaughn, R., Dandass, Y.S., 2011. A testbed for SCADA control system cybersecurity research and pedagogy, in: Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research. p. 27.
Mühlböck, M., Rittberger, B., 2015. The Council, the European Parliament, and the paradox of inter-institutional cooperation. Eur. Integr. Online Pap. EIoP 19.
Olesen, N., 2016. European Public-Private Partnerships on Cybersecurity-An Instrument to Support the Fight Against Cybercrime and Cyberterrorism, in:

Akhgar, B., Brester, B. (Eds.), Combatting Cybercrime and Cyberterrorism. Springer, pp. 259–278.
Olukotun, D., Micek, P., 2016. Five years later: the internet shutdown that rocked Egypt. Access Now.
Orren, K., Skowronek, S., 1996. Institutions and intercurrence: theory building in the fullness of time. Nomos 38, 111–146.
Peters, B.G., 2005. Institutional Theory in Political Science: The "New" Institutionalism. Continuum.
Pierson, P., 2000. Increasing Returns, Path Dependence, and the Study of Politics. Am. Polit. Sci. Rev. 94, 251–267. doi:10.2307/2586011
Pierson, P., 1996. The Path to European Integration A Historical Institutionalist Analysis. Comp. Polit. Stud. 29, 123–163.
Pierson, P., 1995. Fragmented Welfare States: Federal Institutions and the Development of Social Policy. Governance 8, 449–478. doi:10.1111/j.1468-0491.1995.tb00223.x
Pierson, P., Skocpol, T., 2002. Historical institutionalism in contemporary political science, in: Katznelson, I., Milner, H.V. (Eds.), Political Science: The State of the Discipline.
Pollack, M.A., 2007. The New Institutionalisms and European Integration (The Constitutionalism Web-Paper No. p0031). University of Bath, Department of European Studies and Modern Languages.
Pollack, M.A., 2006. Rational choice and EU politics.
Pollack, M.A., 2005. Theorizing the European Union: international organization, domestic polity, or experiment in new governance? Annu Rev Polit Sci 8, 357–398.
Purser, S., 2014. Standards for cyber security, in: Hathaway, M. (Ed.), Best Practices in Computer Network Defense: Incident Detection and Response. pp. 97–106.
Reding, V., 2012. Speech by Vivane Reding: The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age.
Rid, T., 2013. Cyber War Will Not Take Place. Hurst, London.
Robinson, N., 2014. EU cyber-defence: a work in progress (No. 10), EUISS Brief. EUISS, Paris.
Robinson, N., 2013. The European Cyber Security Strategy: Too Big to Fail? | RAND [WWW Document]. URL http://www.rand.org/blog/2013/02/the-european-cyber-security-strategy-too-big-to-fail.html (accessed 11.18.15).
Robinson, N., 2012. European Cybersecurity Policy, in: Andreasson, K.J. (Ed.), Cybersecurity: Public Sector Threats and Responses. CRC Press.
Rosamond, B., 2000. Theories of European Integration, The European Union Series. Macmillan, London.
Rozée, S., 2013. The European Union as a Comprehensive Police Actor, in: Kaunert, C., Leonard, S. (Eds.), European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe. pp. 40–64.
Rudestam, K.E., Newton, R.R., 2014. Surviving Your Dissertation: A Comprehensive Guide to Content and Process: A Comprehensive Guide to Content and Process. Sage Publications.
Russian Federation, 2013. Basic Principles for State Policy of the Russian Federation in the Field of International Information Security (National Strategy).
Samuelson, P., 1996. US Digital Agenda at WIPO, The. Va J Intl L 37, 369.

Sarma, S., 2016. Cyber Security Mechanism in European Union.
Scharpf, F.W., 1997. Games Real Actors Play. Actor-Centered Institutionalism in Policy Research. Boulder, Colo. Westview Press.
Schmidt, A., 2013. The Estonian Cyberattacks, in: Healey, J. (Ed.), A Fierce Domain: Conflict in Cyberspace 1986-2012. CCSA, USA, pp. 174–193.
Schmitter, P.C., 2004. Neo-neofunctionalism. na.
Schwartz, A.J., 2009. Origins of the financial market crisis of 2008. Cato J 29, 19.
S&D, n.d. About us [WWW Document]. Us. URL http://www.socialistsanddemocrats.eu/about-us
Seale, C., 1999. Quality in qualitative research. Qual. Inq. 5, 465–478.
Segell, G.M., 2010. Intelligence agency relations between the European Union and the US. Int. J. Intell. Counterintelligence.
Shiller, R.J., 2012. The subprime solution: How today's global financial crisis happened, and what to do about it. Princeton University Press.
Sikkink, K., Risse, T., 1999. The socialization of international human rights norms into domestic practices, in: The Power of Human Rights: International Norms and Domestic Change. Cambridge University Press, pp. 1–38.
Simões, P., Cruz, T., Proença, J., Monteiro, E., 2015. Specialized Honeypots for SCADA Systems, in: Lehto, M., Neittaanmäki, P. (Eds.), Cyber Security: Analytics, Technology and Automation, Intelligent Systems, Control and Automation: Science and Engineering. Springer International Publishing, pp. 251–269.
Skocpol, T., 1979. States and social revolutions: A comparative analysis of France, Russia and China. Cambridge University Press.
Sliwinski, K.F., 2014. Moving beyond the European Union's Weakness as a Cyber-Security Agent. Contemp. Secur. Policy 35, 468–486.
Smith, M., 2015. The EU as an International Actor, in: Richardson, J., Mazey, S. (Eds.), European Union: Power and Policy-Making. Routledge.
Smith, R.M., 1988. Political Jurisprudence, The "New Institutionalism," and the Future of Public Law. Am. Polit. Sci. Rev. 82, 89–108. doi:10.2307/1958060
Staab, A., 2013. The European Union explained: institutions, actors, global impact. Indiana University Press.
Steinmo, S., 2008. What is Historical Institutionalism, in: Approaches in the Social Sciences. Cambridge University Press, pp. 118–138.
Switzerland, 2012. National Strategy for Switzerland's Protection against Cyber Risks (National Strategy).
Tarrow, S., 2010. Bridging the Qualitative-Quantitative Divide, in: Brady, H.E., Collier, D. (Eds.), Rethinking Social Inquiry: Diverse Tools, Shared Standards. Rowman & Littlefield Publishers, pp. 101–110.
Taylor-Gooby, P.F., 2004. New risks, new welfare: the transformation of the European welfare state. Oxford University Press.
Telephone Interview, Christou, University of Warwick, G., 2014. Interview - Cyber Security and the European Union (PhD) (Warwick University).
Telephone Interview, Kelam MEP, T., 2014. Interview - Cyber Security and the European Union (PhD).
Thelen, K., 2002. The explanatory power of historical institutionalism, in: Mayntz, R. (Ed.), Akteure-Mechanismen–Modelle. Zur Theoriefähigkeit Makro-Sozialer Analysen. Campus Verlag, Frankfurt, pp. 91–107.
Thelen, K., 1999. Historical institutionalism in comparative politics. Annu. Rev. Polit. Sci. 2, 369–404.

Thelen, K., Steinmo, S., 1992. Historical Institutionalism in Comparative Politics, in: Steinmo, S., Thelen, K.A., Longstreth, F. (Eds.), Structuring Politics: Historical Institutionalism in Comparative Analysis, Cambridge Studies in Comparative Politics. Cambridge University Press, Cambridge.

TNS Opinion & Social, European Commission, 2012. Special Eurobarometer 390 Cyber Security Report (No. 390).

Tsagourias, N., 2012. Cyber attacks, self-defence and the problem of attribution. J. Confl. Secur. Law 17, 229–244.

UK, 2011. The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world (National Strategy). UK Cabinet Office.

United Kingdom, 2010. The national security strategy - a strong Britain in an age of uncertainty - Publications - GOV.UK [WWW Document]. URL https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty (accessed 8.19.13).

USA, 2011a. International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World (National Strategy). The White House.

USA, 2011b. Department of Defense Strategy for Operating in Cyberspace (National Strategy). Department of Defense.

USA, 2010. National Security Strategy (National Strategy).

Valeriano, B., Maness, R.C., 2015. Cyber War Versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press.

Verdun, A., 2015. A historical institutionalist explanation of the EU's responses to the euro area financial crisis. J. Eur. Public Policy 22, 219–237. doi:10.1080/13501763.2014.994023

Verdun, A., 2013. Decision-Making before and after Lisbon: The Impact of Changes in Decision-Making Rules. West Eur. Polit. 36, 1128–1142. doi:10.1080/01402382.2013.826021

Verdun, A., 2007. A historical institutionalist analysis of the road to Economic and Monetary Union: a journey with many crossroads, in: Meunier, S., McNamara, K.R. (Eds.), Making History: European Integration and Institutional Change at Fifty, The State of the European Union. p. 195.

Weiss, R.S., 1995. Learning From Strangers: The Art and Method of Qualitative Interview Studies. Simon and Schuster.

Wendt, A., 1995. Constructing international politics. Int. Secur. 71–81.

Wiener, A., Diez, T. (Eds.), 2009. European integration theory. Oxford University Press Oxford.

Young, A.R., 2010. The Single Market, in: Wallace, H., Pollack, M.A., Young, A.R. (Eds.), Policy-Making in the European Union, The New European Union Series. Oxford University Press, Oxford.

Zanders, J.-P., 2009. Cyber Security: What Role for CFSP? (Institute Report No. IESUE/SEM(09)04). European Union Institute for Security Studies.

Zwolski, K., 2013. The European Union and International Security: Developing a Comprehensive Approach, in: Kaunert, C., Leonard, S. (Eds.), European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe. p. 17.