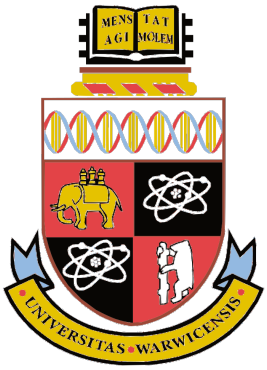
Transatlantic Collaboration in Response to Cyber Crime

How does strategic culture affect EU-U.S. collaboration in the fight against cyber crime?

By Eva Nagyfejeo

MSci (Hons) International Relations and Global Issues, The University of Nottingham

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Politics and International Studies



The University of Warwick

Department of Politics and International Relations

September 2016

Table of Contents

Acknowledgements

I would like to express my sincere thanks and heartfelt gratitude to my supervisors, ***Professor Richard J. Aldrich*** and ***Professor George Christou*** for their patient supervision, invaluable support, guidance and encouragement throughout my research and for allowing me to grow as a research scientist. It has been a pleasure, an amazing privilege and honour to have both of you as my mentors. Without your precious support it would not be possible to conduct this research.

In the U.S. many thanks go to ***Professor Erik Voeten*** at Georgetown University's Edmund A. Walsh School of Foreign Service and Government Department, Washington, D.C., for sponsoring my visiting scholarship. Appreciation and specific thanks also go to ***Professor Catherine Lotriontе***, ***Professor Tim Watson*** and ***Dr Agnes Hankiss***, among many others, for their continued inspiration and helpfulness.

During my fieldwork in Brussels and The Hague I was also warmly received by a number of institutions and organisations therein, all of who were incredibly helpful in connecting me to others in the field of cyber security. My sincere thanks also go to Europol's EC3 Outreach and Support Team who provided me an opportunity to join their team as an intern.

Thanks also go to the interviewees, and to everyone else I have consulted when constructing this study. I would also like to thank all of my friends, fellow students and colleagues from the EU Parliament for their constant encouragement to strive towards my goal.

Special thanks to my family for their financial and emotional support throughout my research. Words cannot express how grateful I am to my mother and father for all of the sacrifices that you have made on my behalf.

Last, but not the least, a great thanks to the staff of the Department of Politics and International Relations for their constant assistance throughout my research at the University of Warwick.

Declaration

This thesis has not been submitted for a degree at another university and is the sole work of the candidate.

Inclusion of Published Work

Some sentences from the book chapter I have published in 2015 and from my master thesis written in 2012 are included in chapters 3, 4 and 5 (please see below).

Publication:

Nagyfejeo, E. (2015) Transatlantic collaboration in countering cyber terrorism. In L. Jarvis, S. MacDonald, T. M. Chen, (Eds.). *Terrorism online*. Abingdon, Oxon; New York, NY: Routledge, pp. 144-172.

Master thesis:

Nagyfejeo, E. (2012) 'European cyber security challenges: why is the European Union unable to develop a joint approach to cyber security?', Master thesis, School of Politics & International Relations, University of Nottingham.

Abstract

This thesis takes Marieke de Goede's intriguing hypothesis on counterterrorism as a starting point. She argues that despite the fact that the general strategic cultures of the European Union (EU) and the United States of America (U.S.) look different on the surface, nevertheless the pre-emptive approach, which is often associated with the U.S., is also deeply rooted in European history. Indeed, most authors agree that there has been considerable convergence behind the scenes on transatlantic counterterrorism. Accordingly, this study attempts to establish whether we can draw similar conclusions regarding EU and U.S. behaviour in the realm of cyber security. The main focus is cyber crime and this is analysed through the lens of strategic culture.

The study examines how far varying attitudes, shaped by strategic culture, hinder the process of cooperation. Moreover, it suggests that an extended version of strategic culture may serve as an alternative tool to aid our understanding of EU and U.S. approaches to fighting cyber crime, at both strategic and operational levels. Currently, there is no literature on fighting cyber crime collaboratively employing a strategic culture approach.

This thesis rejects the argument that there is a single, overarching strategic cyber culture that characterises both the U.S. and the EU. However, it offers the following propositions:

1. The presence of several strategic cyber cultures, within both the U.S. and the EU, creates fragmentation in collaboration.
2. Fragmentation is a partial product of various state and sub-state entities that often do not have a clear understanding of their roles in cyber security, which creates overlaps and disparities in power, thereby generating individual and diverse approaches and attitudes to counter cyber crime.
3. Treating the U.S. government as a 'monolithic' entity, especially with regard to cyber crime policy is a misapprehension. It may be that the growing alignment of U.S. and EU policies originates from the fact that agencies, such as the State Department or DHS, take a decidedly less militaristic approach towards cyberspace, which is a view that aligns more closely with the EU.
4. There is clearly much more convergence in collaboration at the operational level, where there are similar attitudes (U.S. agencies trust each other less than their European counterparts). By contrast, attitudes at the strategic level, together with legal incompatibilities, frequently hinder joint inquiries.

These findings draw heavily upon semi-structured interviews with cyber security officials, politicians, former officials, law enforcement agents and cyber consultants from the private sector. This provides a unique insight into current EU and U.S. security community approaches to the threat of cyber crime, including their mind-set, strategic behaviour and decision-making procedures.

List of Abbreviations

The following list table lists the various abbreviations and acronyms used throughout the thesis.

Abbreviation	Meaning
AFSJ	Area of Freedom, Security and Justice
AGs	Advisory Groups
ANSSI	French Network and Information Security Agency
APT	Advanced Persistent Threats
ATF	Bureau of Alcohol, Tobacco and Firearms
AUSAs	Assistant U.S. attorneys
AUSMIN	Australia-United States Ministerial Consultations
BBC	British Broadcasting Corporation
BBK	Federal Office of Civil Protection and Disaster Assistance (Germany)
BIS	Department for Business, Innovation and Skills (UK)
BKA	Bundeskriminalamt (German Federal Criminal Police Office)
BND	Germany's National Intelligence Agency
BSA	Business Software Alliance
BSI	Bundesamt fuer Sicherheit in der Informationstechnik (German Federal Office for Information Security)
BTWC	Biological and Toxin Weapon Convention
BW	Biological Warfare
C&C	Center Command and Control
C3	US Immigration and Customs Enforcement (ICE) Cyber Crimes
CA	Competent Authority
CALEA	Communications Assistance for Law Enforcement Act
CCIPS	Computer Crime and Intellectual Property Section
CDM	Continuous Diagnostics and Mitigation
CEPOL	European Police College
CERT-EU	Computer Emergency Response Team – European Union
CERTs	Computer Emergency Response Teams
CFAA	Computer Fraud and Abuse Act
CFSP	Common Foreign and Security Policy
CHIP	Computer Hacking and Intellectual Property
CIA	Central Intelligence Agency
CIIP	Critical Information Infrastructure Protection

CIP	Critical Infrastructure Protection
CIs	Critical Infrastructures
CISA	Cybersecurity Information Sharing Act
CISPA	Cyber Intelligence Sharing and Protection Act
CIWIN	Critical Infrastructure Warning Information Network
CJEU	Court of Justice of the European Union
CNCI	Comprehensive National Cyber Security Initiative
CNI	Critical National Infrastructure
COE	Council of Europe
COMSEC	Communications Security
COPPA	Children's Online Privacy Protection Act
CPR	Cyberspace Policy Review
CPU	Central Processing Unit
CSDP	Common Security and Defence Policy
CSE	Child Sexual Exploitation
CSIRTs	Computer Security Incident Response Teams
CSIS	Centre for Strategic and International Studies
DARPA	Defence Advanced Research Projects Agency
DDoS	Distributed Denial-of-Service
DES	Data Encryption Standard
DHS	US Department of Homeland Security
DIA	Defence Intelligence Agency
DNS	Domain Name System
DoD	US Department of Defense
DoJ	US Department of Justice
DPA	Germany's data protection authority
EC3	European Cyber Crime Centre
EC3AA	European Cyber Crime Centre Academic Advisory Network
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECTEG	European Cybercrime Training and Education Group
EDA	European Defence Agency
EDU	Europol Drug Unit
EEAS	European External Action Service
EEC	European Economic Community
EFF	Electronic Frontier Foundation
EJN	European Judicial Network
EMAS	Europol Malware Analysis System
EMPACT	European Multidisciplinary Platform Against

	Criminal Threats
ENISA	European Network and Information Security Agency
EO	Executive Order
EP	European Parliament
EPCIP	European Programme for Critical Infrastructure Protection
ESDP	European Security and Defence Policy
ESP	Electronic Service Provider
ESS	European Union's Security Strategy
ETL	ENISA Threat Landscape
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCTF	European Union Cybercrime Task Force
EUGS	EU Global Strategy on Foreign and Security Policy
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISMA	Federal Information Security Act
FS-ISAC	Financial Services - Information Sharing and Analysis Center
FVEY	Five Eyes intelligence alliance
GAO	Government Accountability Office
GCHQ	Government Communications Headquarters
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GDR	German Democratic Republic
HIPAA	Health Insurance Portability and Accountability Act
HRW	Human Rights Watch
HSI	Homeland Security Investigations
ICANN	Internet Corporation for Assigned Names and Numbers
ICE	Immigration Customs Enforcement
IG	Internet Governance
iOCTA	Internet Organised Crime Threat Assessment (Europol)
IoT	Internet of Things
IP	Intellectual Property
IP	Internet Protocol
IS	Islamic State
ISEC	Prevention of and Fight against Crime

ISPs	Internet Service Providers
IT	Information Technology
IWF	Internet Watch Foundation
J-CAT	Joint Cybercrime Action Taskforce
JITs	Joint Investigation Teams
LE	Law Enforcement
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MaaS	Malware-as-a-Service
MEP	Member of Parliament
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
MoU	Memorandum of Understanding
MS	Member States
NATO	North Atlantic Treaty Organization
NCA	UK National Crime Agency
NCCIC	US National Cybersecurity and Communications Integration Center
NCFTA	National Cyber-Forensics & Training Alliance
NCIJTF	US National Cyber Investigative Joint Task Force
NCIRC	NATO Computer Incident Response Capability
NCRD	(German) National Cyber Response Centre
NIIA	National Information Infrastructure Act
NIPC	National Infrastructure Protection Centre
NIS	Network and Information Security
NIST	US National Institute of Standards and Technology
NSA	US National Security Agency
OECD	Organisation for Economic Cooperation and Development
OECD	Organisation for Economic Cooperation and Development
OHQ	Operational Headquarters
OIA	Office of International Affairs (Department of Justice)
OIG	Office of the Inspector General
OLAF	European Anti-Fraud Office
OLP	Ordinary Legislative Procedure
OMB	Office of Management and Budget
OPEC	Organization of the Petroleum Exporting Countries
OPM	Office of Personnel Management

P2P	Peer-to-Peer
PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
PCCIP	Presidential Commission on Critical Infrastructure Protection
PDD	Presidential Policy Directive
PDD	Presidential Decision Directive
PLA	People's Liberation Army
PNR	Passenger Name Record
PPP	Public-Private Partnerships
PuP	Public-Public
RAT	Remote Access Tool
RCS	Remote Control System
SaaS	Software as a Service
SC	Strategic Culture
SGDSN	General Secretariat for National Defence and Security
SIGINT	Signals Intelligence
SOWI	Bundeswehr Institute of Social Sciences
TCSEC	Trusted Computer System Evaluation Criteria
TFTP	Terrorist Finance Tracking Program
TFTS	Terrorist Finance Tracking System
TOR	The Onion Router
TTIP	Transatlantic Trade and Investment Partnership
TTPs	Tactics, Technologies and Procedures
UK	United Kingdom
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
US	United States
US-CERT	United States - Computer Emergency Response Team
USB	Universal Serial Bus
USC	United States Code
USCYBERCOM	United States Cyber Command
USSS	United States Secret Service
USSTRATCOM	US Strategic Command
WGCC	Working Group on Cyber Security and Cyber Crime

List of Illustrations

The following lists contain any tables and/or figures and illustrated materials included in the thesis.

Chapter I.

Relevance of strategic culture in relation to cyber crime

'On the ground of intersecting highways, join hands with your allies.'
(Sun Tzu on the Art of War)

1. Introduction

The world labours under a misapprehension. It believes that the Internet revolution has happened. In reality it has only just begun. Today 2.9 billion people are connected online, mostly in Europe and in the United States (U.S.), while in many other regions access is low. The lowest level of Internet access is in sub-Saharan Africa at less than 2% (U.N., 2015). Yet this is changing and in the next five years it is estimated that 7.6 billion people will be connected to the Internet, led by Asia then South America and finally Africa (Oerting, 2014; U.N., 2015). Meanwhile, across the "Global North" many non-communication devices will be connected to the Internet, the so-called "Internet of Things." By 2020, everything we buy in shop that costs more than 20 Euros will most likely have an IP address and will be collecting data, sharing it over the Internet, changing the world we live in forever.

Will it be a better world? While everybody enjoys the growing benefits of connectivity as the Internet makes our life ever more convenient and cost-efficient, ordinary users somehow tend to forget about the fact that it is not only 'nice' users who draw advantage from this interconnectedness, but also criminals that lurk unseen. The Internet certainly offers us huge advantages and even transformative power in many areas of our lives, but it comes with risks that are related to the *political economy of communication.* Everybody wants to exploit the benefits of efficacy but

no-one wishes to pay the costs of security, which largely manifest themselves in terms of time and effort. Instead they largely prefer to ignore the dangers of criminals hiding anonymously behind computers in another part of the world.

Crime has gone digital. The more devices connected to the Internet, the more crimes will be committed online. Perennially, law enforcement agencies, governments and industry seem to be lagging behind the criminals who can easily find new and subtler ways to penetrate the system. Each new innovation offers the criminals fresh exploits. Anyone working in the digital security industry is fully aware that there will never be 100% security and it is not only because of the slow development of security technologies. The ubiquitous nature of new software and hardware tools designed to enhance Internet security measures is itself the subject of intense study by criminals who can quickly counteract these measure in order to make money by malicious means, finding the loopholes open to exploitation.

There is still no universally accepted definition of cyber crime. Some view it as a form of crime specifically enabled by cyber – others view it as normal crime that migrates to the Internet. There are many definitions spread out along a continuum, but the underlying reasons for the absence of such a definition can be explained by the many and various different perceptions, together with the lack of agreement on the core characteristics of cyber crime, which are not unlike the endless search for a definition of "terrorism" (Lagazio et al., 2014: 1). But unlike terrorism, cybercrime is a new field and as yet we still only have a limited picture of the whole cyber crime issue, not to mention the complex economic and social consequences. Accordingly, the theoretical and conceptual literature on cyber crime is at present poorly developed.

Nevertheless, there have been important legal advances. The Budapest Convention on Cyber Crime (2001) was the first international treaty on cyber crime that aimed to harmonise national legislation, seeking to encourage a common approach and to foster international collaboration. It has been ratified by 41 countries and signed by 11 others (Council of Europe). This convention can be considered to represent the first positive first step in a new realm, since few nations or organisations adopt the same approaches to combat cyber crime. Inevitably, some of them are better prepared, in other words, 'secured' against crimes committed online, than others. Furthermore, the actors involved in the fight against cyber crime have notably different levels of experiences and skills. Therefore, while each stakeholder knows only a small part of this 'puzzle', and understandably might be reluctant to share the information they know due to fear of indefinable costs, including loss of reputation, the collective cost is fragmentation and loss of collaborative momentum. Indeed, this fragmentation can have a 'poisonous' effect when it comes to collaboration against cyber crime, since collective action is crucial and no single country or nation can tackle the phenomenon alone (Lagazio et. al, 2014: 1-2).

Over the last twenty years we have witnessed a growing conviction that culture matters in international security. One of the areas of emerging consensus is that most countries generate a collective or corporate memory of their recent security experiences that allows some policy learning and shapes their future decisions. This doctoral thesis builds upon the reasonable assumption that there is some divergence in strategic culture between the United States (U.S.) and the European Union (EU). This suggests that in the cyber security context, strategic culture as a concept might be

usefully extended to consider the strategic/policy, legal and operational dimensions of cyber in order to understand to what extent transatlantic practices against cyber crime diverge or else converge. Therefore, the purpose of this research is to interrogate the drivers of various strategic cyber cultures within the U.S. and the EU that determine the way they approach the emerging fight against cyber crime. At a more theoretical level it also seeks to consider how far we can talk about "strategic cyber cultures" and how they are shaped. Likewise, the very presence of various strategic cyber cultures might well be considered to constitute a serious obstacle to our efforts to develop *trust* among stakeholders in a globalised world in which everybody is subject to the same currency in terms of Internet protocols and security resources. The contention advanced by this research is that the different mind-sets, rooted in strategic culture, have real world consequences for state and indeed sub-state behaviours when we seek to collaborate to combat cyber crime. The strategic culture approach is tested here in the context of the U.S.-EU partnership in the fight against cyber crime in order to examine its impact upon collaboration. Meanwhile, the reason why I have elected to place the transatlantic partnership at the 'heart' of this thesis lies in the fact that both the U.S. and the EU are at the forefront of shaping cyberspace with transatlantic cyber crime cooperation, constituting one of the alliance's most successful security platforms. Nevertheless, there is still no current literature written on cyber crime from a strategic culture perspective.

Inevitably perhaps, this thesis is going to have some limitations, as cyberspace is not determined by geographical boundaries, even those employed by important entities such as the U.S. and the EU. While the transatlantic context is undoubtedly important, perhaps even pre-eminent, it may also miss out the way cyber crime and cyber threats

are produced differently in other areas of the world. For instance, cyber crime is increasingly a component of Middle-Eastern and Asian understandings of security. Moreover, from the point of view of the attacker at least, there will be some cross over into these regions as cyber threats are increasingly conceived of in Europe and the U.S. as transcending borders and operating from areas outside their national territory. Nevertheless, a deeper understanding of U.S.-EU behaviour in cyberspace from a cultural-strategic point of view can serve as a useful pathway to analysing the challenges or misconceptions in this realm, while mapping out a common ground where interests and approaches often collide. Moreover, if we understand the driving strategic cultural "forces" that shape U.S. and EU attitudes in the fight against cyber crime, this can perhaps serve as a cultural 'compass' for analysing more elaborate collaboration with other countries including the BRICS countries: Brazil, India, China and Russia.

Furthermore, a key aspect of the successful collaboration against cyber crime lies in effective information sharing that might well be called the "intelligence dimension" of cyber-security. Efficiency in this sensitive realm of alliance collaboration depends on efforts to create a common 'culture' that according to Occhipinti can be considered the 'final building block' that defines to what extent the actors are *willing to share* critical security information (Occhipinti, 2013: 179). Often, the 'will to share' criminal intelligence or sensitive security data can be linked to the philosophies, attitudes, interests and organisational approaches of global actors (Occhipinti, 2013: 183).

The whole texture of transatlantic relations after 9/11 is contested by leading scholars. According to Rees we can observe two phenomena. First, a realisation of the gaps present in U.S. homeland security and therefore, the need to invest more in the emerging field of the international politics of domestic security through seeking alliances: second, the offensive use of military power unilaterally, often ignoring the European allies in operational missions (Rees, 2011: 31). However, others argue that despite these tensions, at a meta-level, following the 9/11 attacks there was a general shift towards greater collaboration on internal security matters that resulted in transatlantic policy convergence, evidenced by judicial cooperation such as the liaison and data sharing agreements between Europol and American law enforcement authorities, or concerning extradition and mutual legal assistance issues (Hamilton, 2010: 132).

The EU-U.S. Passenger Name Record (PNR)[1] agreement that was proposed in 2007 is a useful example of both policy convergence and controversy. Despite serious privacy concerns expressed in the European Parliament, an agreement was finally reached on 4th December 2015 by EU interior ministers (Pop, 2015). The main sticking point was intense concern over the length of time specified for the storage of the data: despite the fact that it will be kept for five years, after the first six month police will have to request a court order in order to get the 'exact names, addresses and billing information of air passengers' (Dep. of Justice and Equality, 2015c). Resistance to these measures can be seen as a classic illustration of a clash of strategic cultures, reflecting local experience over long periods of time. Meanwhile, from the point of view of strategic culture, both the January and November 2015 Paris attacks could be

[1] PNR agreement 'refers to data collected for flights into and out of the EU, that is also useful for terrorist and criminal threat analysis and for specific investigations' (Hamilton, 210: 134).

regarded as an "external shock" generating a radical change in the EU's strategic culture, undermining its reluctance to pass the PNR agreement. This change of EU strategic culture demonstrates that such exceptional historical moments – like the Paris attacks – trigger a seismic change in otherwise stable strategic policies that were hitherto considered successful (Reiter, 2010).

One former Member of Parliament (MEP) has suggested that 'in order to get Europeans work together we need a "shock", a cyber 9/11 to change the policy-makers' attitudes' (Interview, 2014a). Bisson who also proposes strategic culture as a useful lens through which to view U.S. cyber power, similarly argues that the absence of a "Cyber Pearl Harbor" or an 'external stimuli in the form of cyber national crisis' we are unlikely to see any change in the current American determination to become the dominant cyber power (Bisson, 2014: 57). Yet despite the fact that the U.S. military plays a significant role in cyberspace, it would be wrong to rush to the conclusion, as many have, that all of U.S. cyber security policy is militarised and offensive. Indeed, by contrast, this thesis will argue that it is better to avoid treating the U.S. government as one 'monolithic' entity, particularly with regard to cyber crime policy. The idea of the U.S. militarisation of cyberspace might be accurate in relation to U.S. Cyber Command (USCYBERCOM); however, it does not direct overarching U.S. policy. This analysis will be supported by the examination of other federal agencies (e.g.: FBI) that take a less militaristic view of cyberspace, and which demonstrate more strategic alignment with the EU. But rather like the EU, while we can generalise in outline, there are often multiple cultures even within such large and complex federal entities. Accordingly, we should not speak of one militaristic U.S. strategic cyber culture but rather a fragmented one where both state and sub-state

actors bring their own experiences and ‘mentality’ to bear when dealing with cyber crime.

While the style of cybercrime has changed from decade to decade, we already have a substantive history of nefarious activity with computers. This in turn means we can point to government authorities on both sides of the Atlantic that have more than thirty years’ experience in this realm and by equal turns, significant corporate memory in this area. Countries and institution are therefore developing their own distinct styles and approaches, but given the nature of the Internet, they must co-operate if their security efforts are to be effective. It is this transatlantic convergence that we must now turn.

This chapter will unfold in the following way: it will begin by examining the conceptual struggles of cyber crime - since the lack of clear definitions are one of the causes of the fragmentation of EU – U.S. strategic cyber cultures. The next sections will move on to discuss the complex issues that arise when fighting cyber crime and then provide a brief overview of the historical evolution of cyber crime that helps to build a linkage between history, memory and strategic culture. The final elements of the chapter will explore the non-static nature of strategic culture in the Johnston-Gray debate and suggest that broadening the concept of strategic culture is necessary in order to conceptualise strategic cyber culture in a way that is broader and diverse and therefore not solely limited to the context of defence and military.

2. The conceptual struggles of cyber crime

Definitional problems are not restricted to methodological debates amongst scholars. Practitioners are also engaged in their own struggles to clarify the notion of cyber-crime. Without commonly agreed legal definitions regarding what constitutes cyber crime it is difficult to empower legal and law enforcement authorities to prosecute the cyber crime cases not just regionally but also internationally. Therefore, this research suggests that improved judicial solutions could be regarded as one of the more basic keys in order to enhance collaboration. Since there is no current international collaboration in respect of enforcement there is a clear need for an international law that would be binding in 'practical terms'. However, the difficulty is that it is not in the interest of some of the international players such as Russia or China to come to common agreements. For them it is better to "play" without binding rules and to maintain the current *status quo* with its grey areas. Since the U.S. has the biggest stake in terms of intellectual property (IP) protection (economic security) it is understandable that they have a major interest in setting out international rules of norms and behaviour in cyber space.

Both EU and U.S. policy makers and law enforcement officials face similar definitional challenges when tackling cybercrime and its related threats. Despite the various attempts by legislators and scholars to define cyber crime, there is still no universal definition. Even within the transatlantic area this is problematic and the lack of a precise definition of what we understand the term cyber-crime to convey drives inefficiencies in transatlantic cooperation (Camillo & Miranda, 2011: 2). Indeed, in any detailed comparison of strategic U.S. and EU documents (for example, *EU Internal Security Strategy,* 2010c and *International Strategy for Cyberspace* by the

White House, 2011) it soon becomes clear that although the term 'cyber' is present in these documents, it is rather ill-defined (Camillo & Miranda, 2011: 4). Without precise definitions of what we understand as cyber crime, cyber security and cyber espionage it is difficult to develop effective law enforcement cooperation.

Akcadag is one of many scholars who argues that a key problem that the transatlantic community has to face when it comes to tackling cyber-threats is the lack of an international accepted definition on cyber-crime (Akcadag, 2012: 5). Dahle goes further by claiming that a further important point for consideration would be the ability to distinguish in cases of cyber attacks or cyber espionage, and whether they are committed by a state or non-state actor, since determining the origin of a cyber-attack is often difficult. However, research for this dissertation has suggested that this is more about a reluctance to admit knowledge rather than an absence of knowledge about the perpetrator. Moreover, in cases such as 'Stuxnet' (a virus targeting Iran's nuclear programme) or 'Duqu' (stolen data for intelligence purposes) it was not that difficult to realise that it was conducted by states because of the high cost of developing sophisticated malicious malware to destroy or extract data and information (Dahle, 2012: 3).

The Oxford Internet Institute, working with Sarah Oates, came up with suggestions regarding the taxonomy of cyber crime by distinguishing three clear categories:

a) Traditional crime that involves technology (stealing a laptop) – *amplified traditional crime*

b) Traditional crime that uses technology as a mediating tool (419 scams[2]) – *hybrid crime*
c) Solely technological crime (Distributed Denial-of service "DDoS" attacks) – *virtual crime*
(Fafinski *et al*., 2010: 9).

Therefore, it is important to note that what makes cybercrime different from other crime is the way it is committed. This thesis adopts the approach advanced by Brenner: 'criminals use guns whilst cyber criminals use computer technology'. In other words, these are old crimes committed in new ways, where cyberspace acts as the tool for the criminal (Brenner, 2010: 10). Eugene Kaspersky shares the view that criminals mostly use computers in order to commit traditional crimes (Kaspersky, 2014).

It is also noteworthy that despite the lack of clear definitions in the realm of cyber, there is convergence in the U.S. and EU commitments regarding the enhancement of both external and internal cooperation to harmonise the legal framework for law enforcement prosecutions against cyber criminals; however, law enforcement and judicial activity are only a small part of the transatlantic internal security relationship (Camillo & Miranda, 2011: 4).

Even here, there are a number of factors that could hinder law enforcement cooperation in response to cyber crime: (1) Most of the cyber criminals, when they commit cyber crime, are not under the jurisdiction of the country where the cyber crime occurred. Therefore, international barriers slow down their prosecution and

[2] It is a type of fraud that that tricks the victim to reveal confidential information (for e.g. credit card details) in return for a large sum of money.

identification. (2) Differences in domestic legislation are another barrier when it comes to the issue of arresting cyber criminals because there are countries (for example, Romania and Italy) that do not recognise cyber crime in their domestic legislation. This is one of the core reasons for harmonising national and international regulations that can enhance the effectiveness of cross-border law enforcement collaboration in the prosecution of cyber crime (SOCA, 2013). (3) There is also a general lack of awareness of cyber crime that brings another obstacle to the investigation of both 'pure' cyber crime and 'digitally enabled crime' (UK Home Affairs, 2013).

It is obviously beneficial for both the U.S. and the EU to develop resilience to various threats such as the destruction of communications infrastructure and cyber threats owing to their shared vulnerability. The EU constitutes the most promising partner for the U.S. to work with to develop state cyber preparedness within the transatlantic community, building upon joint contingency planning, strong uncompromised back-up systems and early warning-systems (Lentzos & Rose, 2009). The EU-US Working Group on Cyber Security and Cyber Crime (WGCC) has already been established in 2010 for the purpose of sharing best cyber security principles and exercises, combating cyber crime and enhancing the cooperation between public-private partnerships.

3. Complexities

Finally, several factors are at work that render this field intrinsically complex, ensuring that agreed transatlantic or, *a fortiori*, international agreements and standards are especially hard to achieve. Firstly, what makes fighting cyber crime complex is

that both the public and private sector have to deal with a very sophisticated "market" since many of the larger cyber-criminal groups are careful and highly skilled. However, it is also widely acknowledged among cyber security professionals that there is a steady rise not just in criminal but also in nation-based attacks, and there is a widespread fear that governments' and nations' involvement in cyber attacks is becoming an accepted norm (Gartner Security Summit, 2015). Whereas criminal hackers are focusing on how to gain rapid financial profit, a state-sponsored attack most of the time has a precise goal such as seeking strategic or technical information that could offer disruption at a later stage. Consequently, cyber-crime co-operation actually sits on the boundary between law enforcement and national security.

Secondly, the presence of multiple actors within multiple jurisdictions makes it difficult to enforce cyber crime laws and to track down cyber criminals (Wall, 2003: 9). For more than three decades, federal and state governments have passed numerous laws designed to address criminal activity online - however, most of the laws to tackle criminal acts such as phishing scams, unauthorised access and theft of wireless services that did not exist thirty years ago. Numerous laws have appeared on the statute book, but enforcing them and regulating online behaviour at a work-a-day level is another issue. This also explains why local police departments 'shy away' from investigating and enforcing these crimes, despite the fact that they have created their own cyber crime units.

Thirdly, as a result of the "multiplication effect" that the Internet has, the scale in terms of actors and victims vary across the different levels of analysis and this makes it even more difficult to conceptualise cyber crime and for law enforcement agencies

to protect the potential victims. The actor or actors behind one incident can range from lone wolves to extensive criminal networks or even nation states. As Deibert puts it 'cyber crime moves at the speed of electrons, international law enforcement cooperation moves at the speed of bureaucratic institutions' (Deibert, 2012: 266).

4. Historical evolution of cyber crime

Notwithstanding this, it is worth closing with an analysis of the historical evolution of cyber crime, partly because this addresses the concern about the connection between history, memory and strategic culture. Retired officials that are senior in years now reminisce about 'compusec' and illegal activity on the Internet in the 1980s, giving us some three decades of cyber security culture.

Remarkably, the first articles dealing with the history of *computer crime* – illegal use of computer systems, computer sabotage, computer espionage and computer manipulation - go back to the 1960s (Sieber, 1998: 18). However, *computer crime* in the 1960s and 1970s was different from the *cyber crime* we have to confront today. The Internet did not exist at that time, and central processing units (CPUs) were not interacted with other computers (Brenner, 2010: 10). A typical IBM processor in 1960 cost several million dollars and needed special air-conditioning system - only a select group of technicians and researchers were allowed to use it (Levy, 1984: 1984).

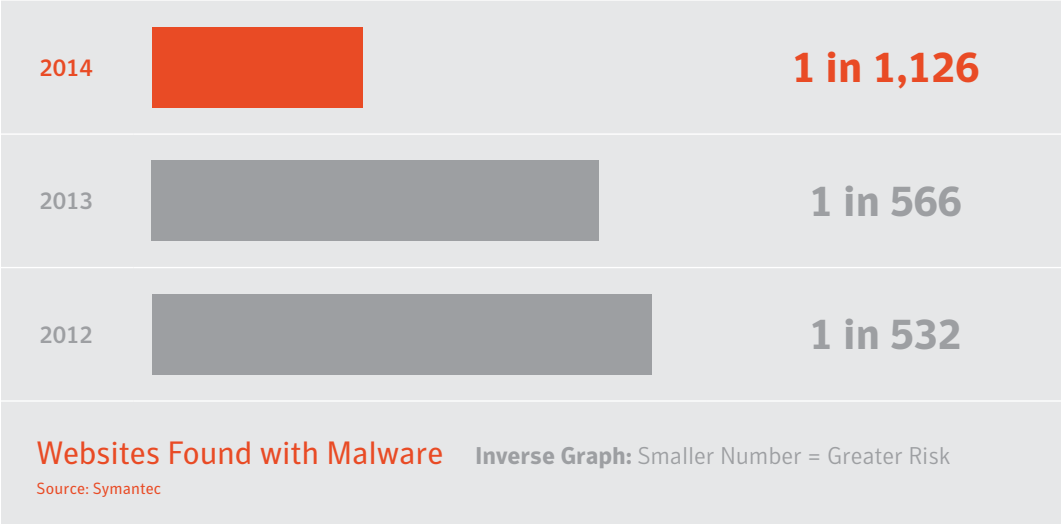
Consequently, only the insiders were in the position to commit cyber crime since they had access to the CPU through their employment (Rasch, 1996). It is widely argued that this also affected the type of computer crimes that were committed in this era such as spying on other employees by reading their confidential files or taking

revenge for being fired by sabotaging a computer or data (McKnight, 1973: 97-112). Nevertheless, the most common computer crime was financial wherein insiders accessed the mainframe computer to gain profit (Brenner, 2010: 11). As a result, all the victims were major enterprises or government agencies because they were the only ones who possessed mainframe computers; and it was not until the 1980s that computers started to be used to actually "harm" individuals as a result of the arrival of the personal computer (Brenner, 2010: 11).

In the 1980s, computer security became a growing concern for the military and struggles for authority often occurred as this new area was fought over between numerous defence and intelligence organisations. Until the 1990s "hacking" was mainly considered to be an intellectual challenge. However, this changed with the arrival of personal computers and the Internet that started to link everything which meant hackers had limitless potential targets and gave rise to a new type of sophisticated criminal with the capacity to exploit both the opportunities and vulnerabilities.

Experts noted that during the growth of cybercrime the *authors* of malware also changed: whilst during the 1990s and early 2000s malware was supposed to be written by adolescent hackers doing it mostly for enjoyment "hacking for sport" (for e.g.: reputation building) however, by 2007 it was possible to observe the "Willie Sutton effect" and malware writing had become the field of professionals – "because that's where the money is" – using it for the purpose of gaining profit such as identity theft, money blackmailing from businesses and holding it encrypted for ransom (Brenner, 2010: 35).

As the authors have changed, so the *tactics* changed as well and it was no longer about sending viruses or worms to the victim's computers anymore. Sophisticated hackers started to "implant" malware in otherwise harmless, legitimate websites and once the individual visited the "infected" website, the computer immediately caught the "infection" without the users' consent (Sophos Security Threat Report, 2008). Despite the fact that in 2014 there was a decrease in the number of websites infected by malware (from 1 in 566 to 1 in 1126) according to the 2015 Symantec Internet Security Threat Report, web threats continue to be considered as one of the biggest challenges for both the public and private sector since cyber criminals are deploying encryption tools more aggressively (Symantec, 2015: 32). Experts say that the reason for the decline can be explained by the growth of web attack toolkits (software as a service "SaaS") designed to exploit the cloud (Symantec, 2015: 41).



[Figure 1.1.]: *Websites found with malware*

(Source: Internet Security Threat Report, 2015, Symantec)

It is interesting to note that according to a 2014 report, *anonymizer* websites have been included in the top 10 most frequently exploited categories of the websites. This

could indicate that since more people are concerned about their browsing privacy and avoid the tracking of the ISPs, the criminals are following the crowd (Symantec, 2015: 39).

Rank	2014 Top 10 Most Frequently Exploited Categories of Websites	2014 Percentage of Total Number of Infected Websites	2013 Top 10	2013 Percentage
1	Technology	21.5%	Technology	9.9%
2	Hosting	7.3%	Business	6.7%
3	Blogging	7.1%	Hosting	5.3%
4	Business	6.0%	Blogging	5.0%
5	Anonymizer	5.0%	Illegal	3.8%
6	Entertainment	2.6%	Shopping	3.3%
7	Shopping	2.5%	Entertainment	2.9%
8	Illegal	2.4%	Automotive	1.8%
9	Placeholder	2.2%	Educational	1.7%
10	Virtual Community	1.8%	Virtual Community	1.7%

Classification of Most Frequently Exploited Websites, 2013–2014

Source: Symantec

[Figure 1.2.]: *Classification of most frequently exploited websites, 2013 - 2014*

(Source: Internet Security Threat Report, 2015, Symantec)

By the year 2000, it had become obvious that with computer technology cyber criminals could commit all sorts of traditional crimes (theft, fraud, IP theft) in new ways and consequently, the scope of criminal law was not sufficient enough and needed to be expanded (Brenner, 2010: 36).

Brenner argues that the U.S. has the most comprehensively advanced cybercrime laws in the world (Brenner, 2010: 49). According to her, the reason for this could be attributed to the fact that the U.S. has been exposed to the challenges of cyber crime to a greater extent compared to others and therefore developed a huge amount of

expertise where each of the 52 U.S. state and the District of Columbia has its own distinct jurisdiction on cyber crime in parallel with the U.S. federal system (Brenner, 2010). As a result of this complexity, legal challenges are present within the U.S., lengthening the process of going to law over cyber in this country.

5. Why strategic culture matters

In 1977, Jack Snyder inaugurated the term *strategic culture* in his RAND research report called 'The Soviet Strategic Culture: Implications for Limited Nuclear Operations'. Since then there has been a growing interest by academics and practitioners in understanding security threats and nation-state responses to security events through the 'lens of culture and national identity' (Snyder, 1977; Lantis, 2002: 87). Snyder argued that the differences between U.S. and Soviet decision-maker's approaches to the use of nuclear weapons could be explained partly by their different cultural and historical beliefs, rather than merely constituting rational actor responses to various scenarios and military technical systems (Snyder, 1977). By examining Soviet deterrence policy, Snyder came to the conclusion that the U.S. had failed to understand and predict Soviet behaviour, often expecting them to react to certain events either as rational actor robots, or else the same way as Americans would do. From his point of view, decisions taken by the political elite on security and military issues represented a distinctive strategic culture backed by the public opinion 'socialised into a distinctive mode of strategic thinking' over a long period of time (Lantis, 2002: 93). In other words, strategic-cultural legacies can play a crucial role in a nation's security behaviour and development of a security policy 'identity'. Searching for an explanation of divergent national 'style' in strategy, many scholars looked to national culture as an escape from behaviourist social science, stating that

each country has its own way to interpret international events and react to them. This was part of a broader pattern that has sought to find a way to give a greater place to ideas as opposed to power in interpreting international security over several decades.

Yet despite more than three decades of extensive scholarly debate on the utility of strategic culture as an analytical concept, there is still no universally accepted single definition of what exactly the core concept of strategic culture is, which factors can activate change in a strategic culture, how it can be measured objectively, how it is supposed to be used academically whether in the national or multinational context and whether it qualifies as a theoretical model (Biehl et al., 2013: 11). Notwithstanding the ambiguities in academic discussions about whether culture matters and whether it can lead to a deeper understanding – even better prediction - of another country's (or adversaries') behaviour, the findings of this research suggest that in the realm of cyber, cultural influence is indeed critical to national policy making.

Culture is perhaps one of the more difficult words in the English language. Nevertheless, it has been embraced with enthusiasm by various social science disciplines, including sociology, anthropology and psychology. Culture has always been a divisive subject when used as an explanation of state performance, partly because the inputs and outputs are often so far apart, and also because the same word is used by many scholars to mean subtly different things. According to Lane & Ersson culture should be understood as the 'identity of communities', a kind of social group that shares either communal values (ethnicity or religion) or universal values (equality or liberty) (Lane & Ersson, 2005: 3). Culture equips individuals with cultural identities that can take the form of ethnicity, religion or universal values. It can also

be used to capture the notion of everyday behaviours and routines that nevertheless signify important underlying ideas and assumptions about the world (Lane & Ersson, 2005: 3).

It was not until the 1960s that the two concepts 'politics and culture' were connected and defined as *political culture* 'a subset of beliefs and values of society that relate to the political system' (Almond & Verba, 1963). Subsequently, it has been widely accepted in academic circles that political culture has both anthropological (language, religion, socialisation) and historical (common memories) foundations that can have an impact on the evolution of political institutions, foreign and security policy doctrines and strategies (Elkiens & Simeon, 1979: 127-128; Lantis, 2002). Sociologist Ann Swidler suggests that culture is a useful set of tools that provides the components (languages, beliefs, stories, ceremonies, habits of everyday life) necessary to develop 'strategies of action' formed by actors (Swidler, 1986: 273). However, one of the main criticisms of culture was its vague descriptive power when confronted with detail and that it gives no clarification about the 'particular choices that individuals make'. This renders it hard for researchers to operationalize (Elkiens & Simeon, 1979: 131).

Yet the original concept of connecting culture with national security policy was already present in outline in the classic works of Sun Tzu, Thucydides and Carl von Clausewitz (Lantis, 2002: 93). 'Know your enemy and know yourself and you can fight a hundred battles without disaster' (Sun Tzu, 1983: 15). Sun Tzu's words suggest that once you understand your enemy's strategic culture, you are already half way to policy success, since you then enjoy a better idea of what might be in the

enemy's head and so better able to predict their plans, or more likely perhaps which options are culturally unattractive to them (Sun Tzu, 1983: 15; Stone et al., 2005).

> Thus it is said that one who knows the enemy and knows himself will not be endangered in a hundred engagements. One who does not know the enemy but knows himself will sometimes be victorious, sometimes meet with defeat. One who knows neither the enemy nor himself will invariably be defeated in every engagement (Sun Tzu, 1983).

Cyberspace is the realm of the unknown enemy. Here, it is very difficult to determine attribution – the source of the attack - and where the enemy is coming from. The number of lone wolf patriot hackers and criminals (that can be of any nationality) is rising steadily year-by-year. The aggressor only needs a computer and some IT skills in order to carry out the malicious attack. Hence, an asymmetric disadvantage already favours the attacker. The likelihood of finding the precise source of the enemy in cyberspace quickly and effectively is rather low and takes up lots of time.

Consequently, Sun Tzu's suggestion to 'know your enemy' – an appeal to leverage strategic culture - might not be easily applied to cyberspace. That is one of the reasons why the U.S. prioritizes offense over defence. Steven Chabinsky, formerly the head of the FBI's cyber intelligence section and now chief risk officer at CrowdStrike, openly stated that: 'There is no way that we are going to win the cyber security effort on defence. We have to go on offense.' (Gjelten, 2013). It is necessary to add that this offensive military mind-set, which is deeply rooted in the strategic-cultural history of the U.S., is not only present in U.S. cyberspace policy but also in many realms of US national security policy including US policy towards militarised space and U.S. foreign policy in the Middle East. Exemplifying this, in September

2014 Obama stated that in order to fight ISIS (Islamic State) the U.S. has started 'going on some offense by using airstrikes to protect American personnel and gathering increased intelligence on ISIS' (Caldwell & McLaughin, 2014).

Broadly speaking, the U.S. way of dealing with security threats originating from terrorism and organised crime has prompted the same reactions to tackle cyber threats in cyberspace. For this reason, the study is going to examine the motivational factors generating strategic responses against cyber threats from nation states, sub-state actors and supranational organisations, comparing two complex actors: the U.S. and the European Union (EU). Responses and approaches vary due to the different geostrategic and cultural positions that nations represent. Nevertheless, a better understanding of the strategic culture of these two key actors and their approaches to tackling cyber threats could identify means to improve this collaboration, or indeed collaboration against cyber crime generally.

5.1. Conceptual struggles over strategic culture

Strategic culture is not a new concept. Within the wider ambit of the strategic culture literature there have been various attempts to conceptualise the term in order to help explain why certain states act the way they do. For instance, a nation's own collective memory of its historical security experience with major threats can determine the way a nation reacts and responds to future security risks and can also influence the type of security strategy a nation develops. To put it simply, recent history, and especially major crises, impact upon the strategic choice a country makes regarding matters such as the use of force or choice of alliance partners (Aldrich & Rees, 2005; Rees, 2011: 31). However, the term 'means different things to different people' and this

illuminates its persistent vagueness (Norheim-Martinsen, 2011: 524). Therefore, not only have scholars failed to agree on a universal definition of strategic culture, but also they have struggled to develop a methodology to study it as a process and to demonstrate how it actually works. There are a variety of unanswered methodological questions: Should strategic culture be used as an independent, intervening or dependent variable? Is it changing or persistent? Who are the carriers of strategic culture? The main intellectual controversies are linked to the question of how far we can operationalise the idea to explain behaviour in detail, captured in the famous Gray-Johnston debate (Gray, 2007:1). Nevertheless, Gray argues this matter of methodology is a problematic issue only for academic theory builders and actually it is not of great importance since it is self-evident that all human beings (including both realists and neorealists) are 'cultural creatures' (Gray, 2006: ii).

One of the most respected scholars working in this area has summarised strategic culture as:

> shared beliefs, norms and ideas within a given society that generate specific expectations about the respective community's preferences and actions in security and defence policy. In this context, a community's security and defence identity, expressed through its preferences and behavioural patterns, derives from shared experiences and accepted narratives specific to a particular security community (Biehl et al., 2013: 12).

Deploying the above definition, strategic culture is understood as the beliefs and assumptions of a specific actor that then acts as a framework, perhaps even a form of constraint, when the individual makes choices in security and defence (Rosen, 1996: 12). Another understanding of strategic culture that commands broad consensus is that it can be understood as 'shared beliefs, assumptions, and modes of behaviour, derived from common experiences and accepted narratives (both oral and written),

that shape collective identity and relationships to other groups, and which determine appropriate ends and means for achieving security objectives' (Johnson & Larsen, 2006: 3). Effectively, this suggests that several different communities of security analysts all represent strategic thinking and behaviours as shaped by distinctive historical experiences and geographical locations. In other words, a security community's own interpretation and education of history and geopolitics impacts the way security actors discuss and react to certain national security threats (Gray, 2006: 7).

A programme of comparative strategic analysis conducted in 2008 at the Bundeswehr Institute of Social Sciences (SOWI), sought to 'unpack' strategic culture and identified four areas that could serve as an indicator regarding a nation's security and defence policies:

a) the level of ambition in international security policy
b) the scope of action for the executive in decision-making
c) foreign policy orientation
d) the willingness to use military force (Biehl et al., 2013: 13).

Mapping and matching U.S. and EU positions in these four areas could be one way of analysing their cooperation in the field of cyber crime. Whilst convergence in one or more dimensions could be a facilitator for closer collaboration, divergence could be a source of stagnation (Biehl et al., 2013: 13). More precisely, memories of past historical episodes and experiences could be regarded as important factors if we wish to benchmark the strategic culture of both the U.S. and the EU in this realm.

All the same, strategic culture theorists Colin S. Gray and Jack Snyder both warn about the pitfalls of explaining the differences between global actors (such as the U.S. and the EU) by simply applying the label of 'culture' (Gray, 1981; Snyder, 1977). Rather like "globalisation", the terms strategic culture risks explaining everything but also explaining nothing. However, it is hard to disagree with the observation made by Ken Booth who argues that that decision-making cannot be completely separated from the context of culture, since elite strategic behaviour is determined by experiences in the past (both historical and security), just as individual human beings learn from experience (Booth, 1990; Toje, 2008:18). As a consequence, the differences in strategic culture could be used as a tool to help to understand some of the misconceptions among strategic actors when they implement different countermeasures to reduce security threats such as cyber crime.

Because strategic culture consists of public, strategic and military identities, it is not static but changeable and adapts drastically to the new circumstances when subjected to collective shocks (Gray, 2006: 11). Accordingly, when a society experiences a serious social, military, political reverse or a disaster, it often embraces new way of thinking relatively easily while simultaneously searching for the answers as to why the shock has occurred. As a result, the community becomes more amenable towards convergence with other cultures they have to collaborate with globally. For example, after the surprise attacks of 9/11, 'the shock of being attacked' was a catalyst for American scholars to re-explore American strategic culture and apply it to policy-making (Kartchner et al., 2009: 6). Precisely in order to raise cultural awareness within U.S. security and foreign policy, the 2004 Report of the Defence Science Board Task Force on Strategic Communications concluded that an in-depth

knowledge on other cultures and factors that influence human behaviour are vital tools in order to develop policies and strategic communications (Department of Defence, DSB, 2004).

With specific regard to cyber-security, the critical issue is that strategic culture is historically constructed and therefore we confront the question of whether one can talk about a meaningful strategic cyber culture in 2016? Whilst some might argue that there is not enough history and what we have is relatively small, in fact its predecessors, "Compusec" and "Infosec" were familiar subjects in the 1980s, with the first email being sent in 1974. Moreover, most NATO countries have a long history of collaboration in areas such as computer export control for defence purposes.

Whilst both the EU and the U.S. share the same basic security assumption that nations are facing new and emerging security challenges when talking about cyber threats, not all experts accept this framing. Some EU officials interviewed for this project insist that these challenges are not new at all because they already existed before under the labels of "compusec", "infosec" and "information assurance". Subsisting under these less dramatic labels, they did not command quite so much attention as pressing issues, but they were nevertheless in existence for more than two decades (Interview, 2014g).

Moreover, Healey argues that in terms of U.S. cyber conflict[3] there is a relevant amount of history but the detailed lessons are often forgotten (Healey, 2013: 16). Healey argues that since the mid-1990s there have been 7 major Cyber Wake-Up Calls (so far):

[3] Healey refers to cyber conflict that excludes most cyber crime conducted for material/criminal motives not for political purpose but includes large malicious Internet disruptions.

1. Morris Worm
2. ELIGIBLE RECEIVER and SOLAR SUNRISE
3. MOONLIGHT MAZE
4. Chinese Espionage
5. Estonia and Georgia
6. BUCKSHOT YANKEE
7. Stuxnet

Healey argues that there are in fact several shared histories of cyber crime that policy makers could rely on and learn from in order to reach their cyber security objectives both in the EU and the U.S. However, the number of cyber crime cases that occurred so far often does not provide sufficient 'corporate memory' of major events for the security community to decode them and develop effective strategic countermeasures in an organic way, or incorporate into wider strategic thinking.

Healey highlighted that even if there were "cyber wake-up calls" that surprised decision makers at the time; the lessons were quickly forgotten until policy makers experienced a similar cyber shock a number of times (Healey, 2013). Whilst there is no definite answer as to why the lessons are not learnt and why policymakers often tend to overlook recent cyber events, depending instead on a more "historical mind-set", one explanation could be that technology is constantly evolving and most policy - legal measures that came into force to counter cyber disruptions that occurred in the past (for instance 5 years ago) might well be irrelevant today. In other words, while decision-makers are often pressured to implement preventative measures in order to avoid future cyber doom scenarios, their strategic culture is constructed from events in the past. Accordingly, strategic culture makes it harder to construct a cohesive cyber security strategy since new military personnel, diplomats and policy makers can only rely on it order to avoid old mistakes or else to construct very broad security doctrine.

Healey provides three explanations as to why lessons of U.S. cyber conflicts are often ignored and do not provide the basis for effective social learning within organisations: The first is linked to those practitioners who see cyber conflicts merely as a narrow technical challenge rather than grasping the whole national security dynamic operating during the cyber conflict cycle. The second factor is connected to those international security practitioners who have a vague idea about cyberspace and therefore have been misinformed about cyber being a new and difficult realm which makes their normal approaches to security difficult to implement. The third factor could be connected to excessive government secrecy, or else corporate confidentiality driven by a desire to maintain business confidence. The latter is especially visible in the banking sector. (Healey, 2013: 16).

5.2. The Johnston-Gray Debate

When talking about strategic culture it is necessary to visit the Johnston-Gray debate that still remains the 'touchstone' of the concept for political scientists keen to use it as research method. Their disagreements in part reflected different purposes, while Gray was interested in more general notions of strategy, Johnston wished to use the idea to explore Chinese behaviour more specifically. Therefore, the main argument was whether to include "behaviour" within the definition or not. When Colin Gray wrote about strategic culture back in 1981 he considered it as a vital tool in order to recognise the different strategic choices made by different national communities (Lock, 2010: 686; Gray, 1981). Gray argues that culture as a framework can provide a better picture of what behaviour means, however there is hardly any discussion about other factors set outside of the strategic culture context (Gray, 1999: 68; Poore, 2003).

Then in 1995, Alistair Johnston came up with categorisations designed to make the concept a more operational tool: meanwhile relegating Gray to the first generation of analysts next to Snyder and criticising them for considering American strategic culture as one, homogenous entity and separately produced from the Soviet strategic culture in the context of war planning (Johnston, 1995: 37). Furthermore, Johnston argues that the first generation approach is vague and inconsistent, falsely claiming that 'strategic culture tends to lead to particular strategic behaviours, or that strategy is in part a product of culture' (Johnston, 1995: 38). According to Johnston, behaviour and culture should be handled independently since behaviour represents only a small 'hegemonistic' group of people (the decision-makers) whose interests are reflected in the strategic choices that nations make (Johnston, 1995: 40). For that reason, Johnston's counterargument against Gray was to emphasise other non-strategic culture variables when explaining behaviour that could be 'tested in the causality in cultural and non-cultural variables in determining outcomes' (Poore, 2003: 281). In other words, Johnston was more confident that the inputs and outputs of strategic culture, although far apart, could be subjected to rigorous testing alongside other possible drivers of behaviour.

Gray's argument is more about style: 'the idea of an American national style (national historical experience, geography, way of life, political philosophy) is derivative from the idea of American strategic culture, suggesting that there is an American way in strategic matters' (Gray, 1981: 22). By contrast, Johnston argues that Gray's view of strategic culture is too restricted to national boundaries and geographical territory. In *Strategic culture revisited,* Johnston states that while analysing Chinese strategic

culture, he paid careful attention to distinguish different 'strategic cultures within specific ethno-territorial space and time' (Johnston, 1996: 522). Nonetheless, Poore is quite suspicious about Johnston's approach which involves testing strategic outcomes by the impact of strategic culture and criticises Johnston for not providing a more detailed explanation for when and why one strategic culture overrides the other (Poore, 2003: 283). Currently, these methodological questions remain one of the biggest headaches for those seeking to generate a theory of strategic culture. Meanwhile, the complexities of finding cultural variables that could be operationalized and clearly defined makes it rather unappealing for academics who want to apply culture as an analytical tool, especially those who wish to make use of quantifiable data (Poore, 2003: 283).

Nevertheless, the Johnston - Gray scholarly debate on whether to conceptually distinguish strategic behaviour from strategic culture, has not slowed the appearance of strategic culture literature and there has been a profusion of writing on the subject. As Gray states, 'the ability of scholars to make a necessarily opaque concept like strategic culture even less penetrable is truly amazing' (Gray, 2006: 9). Both of the approaches have their own merits and much depends on what the concept is used for, especially whether there is a desire to use it qualitatively or quantitatively. Gray's approach remains under-theorised and deterministic while the problem with Johnston's method is there is no suggestion on the way to measure cultural variables (Poore, 2003). Therefore, this debate seems to be linked to wider scholarly conflicts and likely to be resolved only by the injection of new techniques from other disciplines such as sociology or political psychology.

5.3. The three waves of strategic culture

According to Alistair Iain Johnston, the examination of the *strategic culture* concept can be discussed in terms of three generations of writers in the field of international relations and international security studies. This research will also posit a fourth group of representatives of strategic culture analysts that emerged after 9/11.

Based on Johnston's categorisation, the first generation of theories emerged around the late 1970s and early 1980s, the second from the mid-1980s and the third group in the early 1990s (Johnston, 1995). Colin S. Gray, Ken Booth, David Jones next to Snyder represent the '**first generation**' who position the strategic culture debate within the U.S. – Soviet nuclear-strategy nexus and who are all inhabitants of the world of strategic studies which was pre-occupied with the problem of managing the baroque nuclear arsenals that had developed rapidly during the first two decades after the end of the Second World War (Johnston, 1995: 36; Toje, 2008: 15). Gray argues that the American approach to nuclear strategy can be linked to their national historical experiences. According to their national beliefs, a nuclear war was impossible to win, as it would result in an enormous human loss, therefore, the over-arching objective was to preserve American technological superiority so it could act as a nuclear deterrence against the Soviet Union (Gray, 1981: 41; Johnston, 1995: 36). In his later works, Gray describes strategic culture as 'the persisting (though not eternal) socially transmitted ideas, attitudes, traditions, habits of mind, and preferred methods of operation that are more or less specific to a particularly geographically-based security community that has had a necessarily unique historical experience' (Gray, 1999: 51). His sophisticated portrayal of strategic culture supports the idea that historical experience plays a vital role in shaping strategic developments. Ken Booth

can be considered as another security policy scholar echoing Snyder's views in his influential short text: *Strategy and Ethnocentrism* (1979) in which he wrote about a range of ideas, including Groupthink, and their ability to degrade or distort the relationship between coherent nuclear strategy and superpower relations (Kartchner et al., 2009: 35).

As we can see the 'first generation' struggled with the conceptualisation of the term, lacked methodological consistency by arguing that strategic culture indicates only one type of behaviour, meanwhile the puzzle between behaviour and strategic culture remained unresolved. This led to the emergence of the next wave of strategic culture scholars.

Bradley S. Klein and Robin Luckham can be regarded as the forecasters of the '**second generation**' of strategic culture theories. They argued that one needs to make a clear line between behaviour and strategic culture, whilst in reality the selfishness of a small elite hegemonic community drives strategic choices and not a broadly-owned strategic culture (Sondhaus, 2006: 8; Klein, 1988; Luckham, 1984). (This is of some importance to this study, since at a later point we must address whether approaches to cyber security in the EU and US, are defined by a large community that includes corporates and consultants or a small government elite) The proposition of the second wave of theorists is that there is dissimilarity between the way political leaders, the 'elite', claim to act and the hidden intentions behind what they are actually doing (Stone, 2006). Correspondingly, they argue that strategic culture acts as a manipulative 'Machiavellian' instrument for political authorities when strategic decisions are made (Poore, 2003: 284). This can be strongly linked to the dichotomy

of the U.S. declaratory-operational strategies (Klein, 1988: 136, Toje, 2008:17). Hereby, declaratory strategies were actually rhetoric doctrines used by the political elite in order to secure the support of the public and deceive political opponents for the validation of their actions, the real operational strategy (Toje, 2008). Operational strategy by contrast, as part of the U.S. nuclear policy, placed emphasis on defending the interest of American supremacy and ensuring combat-readiness (Johnston, 1995: 39).

However, there are several deficiencies in the arguments of the second generation that inevitably led to the appearance of the next generation. One of the problems with the second generation writing is that the linkage between strategic discourse and behaviour remains blurry. We still do not know whether strategic discourses affect behaviour by taking into consideration the ideas that 'elites' - being the embodiment of strategic culture - could be influenced by 'the symbolic myths' of their ancestors (Stone, 2006: 2). Furthermore, it also avoids taking into consideration how incidents increasingly take place across different countries and alliance systems and therefore whether the differences at cross-national level are present in strategy.

The '**third generation**' arrived in the early 1990s. Johnston considers himself part of this generation, next to Jeffrey Legro and Elizabeth Kier, who is less deterministic compared to the first generation and avoid including 'behaviour' as element of strategic culture as it would militate against their focus on competitive theory testing (Johnston, 1995: 43; Gray, 2007: 3). Kier in her article *Culture and Military Doctrine: France Between the Wars* clearly states that her work is focusing on organisational culture in the military context that 'is not equivalent of a national

character' (Kier, 1995: 67). Likewise Legro in *Military Culture and Inadvertent Escalation in World War II* maintains that when thinking of which type of culture had larger influence on the way wars were fought nationwide, he points to military organisational culture rather than a broader strategic culture, since 'both Germany and Britain had ways of war that worked to suppress inadvertent escalation' (Legro, 1994: 133).

Johnston advances his own idea of strategic culture by claiming a gap between strategic culture and strategic behaviour. Johnston does not come up with a unique definition but borrows the idea from Geertz and conceptualises strategic culture as an 'integrated system of symbols (e.g., argumentation structures, languages, analogies, metaphors) which acts to establish pervasive and long-lasting strategic preferences by formulating concepts of the role and efficacy of military force in interstate political affairs, and by clothing these conceptions with such an aura of factuality that the strategic preferences seem uniquely realistic and efficacious' (Geertz, 1973 :90; Johnston, 1995: 46). Accordingly, this clearly leaves out behaviour as an independent variable. This, is turn, explains why most of the strategic culture scholars locate their own works based on the 'Johnston vs. Gray' debate and why the strategic culture literature is centred on this debate.

In essence, the **third generation** avoids the determinism that is the main characteristic of the **first generation** and is notably devoted to 'competitive theory testing by pitting alternative explanations to each other' (Johnston, 1995: 42). For example, Johnston highlights that Legro understands recent experience as direct influence on culture and contrasts models to each other, typically realist set against

institutionalist approaches. Similarly, Kier follows the same method by comparing 'structural realism, bureaucratic organizational models, and the concept of military culture' (Johnston, 1995: 42). Despite these strengths, there are several shortcomings; such as the inconsistency in handling short-term realism to explain immediate strategic choices or the use of organizational culture as an independent variable. Most alarmingly, the central conceptual framework is still vague (Stone, 2006).

5.4. The fourth (new) wave of strategic culture since 9/11

In the flood of security literature immediately **after 9/11** we can see that work on EU strategic culture has gained saliency despite being a previously under-researched field. Significant studies have been carried out by Howorth (2002, 2007) and Biscop & Coelmont (2011), which attempt to conceptualise strategic culture in various ways and examine how the EU responds to this challenge whilst searching for grand strategy. Meyer (2005, 2006) analyses EU strategic culture from a constructivist angle. Moreover, in 2011 a special issue of the journal *Contemporary Security* was dedicated to Common Security and Defence Policy (CSDP) and strategic culture combining it with several aspects of EU security policy from various theoretical perspectives (Haglund, 2011; Haine, 2011; Kammel, 2011; Norheim-Martinsen, 2011; Pentland, 2011; Peters, 2011; Rynning, 2011a, b; Schmidt, 2011; Schmidt & Zyla, 2011; Zyla, 2011).

Again, we note a strong emerging consensus that culture influences the security policies of countries, but the ambiguity in terms of a universal definition is still a significant issue. Furthermore, the problem is only superficially one of definition, and

lurking below are more complex controversies between various scholars with conflicting views of cultural dynamics and how strategic culture is created and in turn shapes events (Hudson, 1997: 2). To some extent we suffer the travails of inter-disciplinarity here. Since strategic culture covers a variety of disciplines (psychology, sociology, political science, and international relations theory) a definition needs to cover all of these fields, especially when focusing on non-state actors such as personal psychology, symbols and organized cultures. Yet the very richness of the field and variety of social scientists working on the problem means that convergence around a single concept is far from likely (Stone et al., 2005).

Kerry Longhurst might be considered one of the greatest contributors in explaining the impact and dynamic aspects of strategic culture by focusing on three elements: 'regulatory policies, foundational elements and security policy standpoints' (Longhurst, 2004: 17-18). She argues that 'foundational elements' are the main principles regarding the use of force that act as the cornerstone of strategic culture. Basic principles and beliefs are primarily long lasting, highly resistant to change and play a vital role in the development of national identity. Moreover, they demonstrate the core of strategic culture to the external environment by disseminating these foundational elements with long-term policies and practices through channels of meaning and application are called 'regulatory practices' (Longhurst, 2004; Sondhaus, 2006: 128). Somewhere between the 'regulatory practices' and 'foundational elements' are 'the security policy standpoints' that are present-day, commonly agreed understandings on the way core values should be projected across policy channels and therefore, set the direction of policy choices. For this reason, Longhurst suggests that these three elements in motion remind us that that strategic

culture is an ongoing process of constant 'self-evaluation' (Longhurst, 2004: 48). This state of constant change, albeit often incremental, is an essential point for our research and we will return to this issue, in order to apply it to the development of cyber policies.

Similarly, Anja Dalgaard Nielsen, alongside Longhurst is also an advocate of the idea that culture consists of various layers of principles and mind-sets that are subject to different levels of challenge and change. One might posit that strategic cyber cultures are also subject to change. Depending on the level and circumstances, these values and beliefs can become less important to a given culture that is more open to a wider range of inputs and is more broadly owned (Dalgaard-Nielsen, 2006: 13; Longhurst, 2004: 17). The difference between the two scholars concerns what factors can trigger significant change. Longhurst argues that structural changes are the dominant players while Dalgaard-Nielsen favours agency, suggesting that certain situations can influence political initiatives of individuals that alter culture (Daalgaard-Nielsen, 2006: 11). It could be argued that Longhurst's approach provides a 'mediating role' by supporting Snyder's idea that historical foundations and 'pre-existing cultural beliefs' can prompt change in strategic culture, meanwhile refining the concepts of both Booth and Gray 'into something with a degree of structure and greater analytical utility' (Sondhaus, 2006: 128).

It was mentioned previously that communal shocks could drastically alter cultures. Among the post 9/11 scholars, Jeffrey Lantis can be considered to be the scholar offering the most detailed analysis regarding **change in strategic culture** (Pirani, 2014). He argues that the appearance of 'strategic cultural dilemmas', more precisely,

when ‘external shocks fundamentally challenge existing beliefs and undermine past historical narratives’ can be regarded as a sign that political culture may undergo significant change (Lantis, 2002: 111). As a result of such conditions, ‘foreign policy behaviour may break the traditional bounds of strategic cultural orientations when primary tenets of strategic thought directly conflict with one another’ (Lantis, 2002: 112). However, dilemmas of strategic culture could be solved by changes in the national security policy (Pirani, 2014: 2). Exemplifying this, Thomas Berger explains in Katzenstein’s influential edited volume that in the case of Germany and Japan only a ‘major external shock’ could have a drastic impact on their post-1945 cultures of anti-militarism; a similar shock to the major defeat in the Second World War that put an end to their pre-1945 militaristic cultures (Berger, 1998: 209; Sondhaus, 2006: 10, Katzenstein, 1996: 261). By contrast, an external shock might not be the only reason that would trigger a change in a country’s national security policy. To demonstrate this: according to the constitution, at least, Japan is a pacifist country. Article 9 that was introduced after the Second World War stating that ‘The Japanese people forever renounce war and the threat or use of force’. This has been challenged by the new laws that were introduced by Prime Minister Shinzo Abe in September 2015 that would allow the military to fight overseas in collective self-defence – also so called ‘proactive pacifism’ (BBC, Sept. 2015; Choong, 2015).

Longhurst also concluded in *Germany and the Use of Force* that strategic culture is never stagnant but is in a state of constant change wherein these fluxes are thought to be ‘fine-tuning’ rather than ‘fundamental’ (Longhurst, 2004: 17-18). The difficulty although arises when deciding whether a cultural change is ‘fine-tuning’ or ‘fundamental’, or perhaps even something in between (Sondhaus, 2006).

Nonetheless, what distinguishes Lantis from other external shock-theory scholars is his unique way of viewing external shocks not only as an outcome of unique historical events at exceptional moments, but also as fundamental changes in geopolitical situations that can put a country's strategic culture under pressure and trigger the wider transformation of strategic policies (Pirani, 2014: 2). Bisson argues that only a major cyber-attack or cyber war against the United States has the likely chance of changing the current pre-eminence of American cyber power (Bisson, 2014). We might note that, since June 2013, the EU-U.S. collaboration in cyber security has been shadowed by the Snowden revelations (a significant external shock) and has been subject of much debate in Europe, especially Germany. Trust within the transatlantic alliance has been damaged that needs to be rebuilt again. This could be achieved if the transatlantic partnership is based on common social principles and standards. There is clearly a high degree of interest on the U.S. side directed to expand the existing EU-U.S. Cyber Dialogue also on the defence aspects. Perhaps because we are still in the Snowden aftermath, the EU remains quite cautious.

[Table 1.1.]: *Waves of strategic culture*

Waves of Strategic Culture	**Scholars**	**Arguments**	**Limitations**
Wave 1 (Late 1970s and early 1980s)	- Jack Snyder - Colin S. Gray - David R. Jones - Carnes Lord - Kenneth Booth	- Differences between American -Soviet nuclear strategic thinking explained by historical experiences, geography and political culture that leads to a certain type of behaviour - Ethnocentrism is inevitable regarding matters of national	- Vagueness of conceptualising the term - Arguing that strategic culture leads to only one type of behaviour - Missing out the existence of various strategic cultures within one country

		defence	- Assuming the homogeneity of strategic culture across time can be problematic
Wave 2 (Mid 1980s)	- Bradley Klein - Robin Luckham	- Huge difference between what elites are saying will do and what is happening in reality - Elites use strategic culture as a tool to maintain their political hegemony when making strategic choices - Distinction between strategic culture and behaviour; declaratory and secret doctrine	- Relationship between culture and behaviour is still blurry - Problem of measuring the consciousness of elites about the difference between declaratory doctrine and 'real' doctrine - Undecided whether to expect cross-national differences in strategy - It is not applicable for more specific purposes
Wave 3 (1990s)	- Alastair Johnston - Elisabeth Kier - Jeffrey Legro - Ronald Jefferson - Peter J. Katzenstein - Thomas Berger - Alexander Wendt	- Circumvents the determinism of the first generation - Treats strategic culture as an independent variable whilst behaviour as a dependent variable - Committed to competitive theory testing - Contrasting the cultural explanation of behaviour against alternative explanations such as realist and institutionalist ones	- The definition is still loose - Problem of focusing on realism weaknesses - Lacks acknowledging that culture overlaps with other entities of the same kind in various ways - Using organisational culture as a key independent variable in strategic choices is problematic
Wave 4 (Post 9/11)	- Jeffrey Lantis - Elisabeth Stone - Kerry Longhurst - Anna Dalgaard-Nielsen - Henrikki Heikka	- Theorising culture as an interplay between discourse and practice - Stressing the dynamic aspect of culture - Focusing on change and continuity - External shocks can	- Lack of a detailed analysis of the link between culture and framing - Still no answer whether the motivation that drives the elite is

	- Iver B. Neumann - David McCraw - Alan Bloomfield - Christoph Meyer - Asle Toje - Mary N. Hampton - Theo Farrell - Schmidt & Zyla - Biscop & Coelmont	generate strategic cultural dilemmas resulting in the change of political culture - Elite actors are portrayed as 'users of culture' who consciously manipulate foreign and security policy behaviour	rooted in the cultural environment or it is determined by other external factors

Source: Based on and updated from Elisabeth Stone, Comparative strategic cultures, 2006

6. Conceptualising strategic cyber culture

Scientists suggest that by 2025 we will have seventy-five billion devices connected to the Internet – the so-called "Internet of Things". The more devices that are connected to the Internet, the more crimes will be committed online. Law enforcement agencies, governments and industry are lagging behind the criminals who often find new and subtle ways to penetrate the associated systems. These criminals increasingly operate globally, exploiting gaps between jurisdictions, making international co-operation ever more important. Therefore, this research aims to respond to a lacuna in the literature by analysing EU-U.S. collaboration in the fight against cybercrime by deploying a widely respected body of theory in the field of IR, the idea of strategic culture. Using this prism, it will probe the drivers of convergence and divergence, together with the strengths and weaknesses of this important collaboration.

Despite the fact that strategic culture still remains somewhat under-theorized and remains an area of contestation, especially in terms of method, this study accepts that any IR approach that deals with the slippery territory of ideas, norms and cultures is likely to involve methodological worries for those intent on measuring inputs

precisely. Notwithstanding these anxieties, the following section is going to discuss why strategic culture could be used as an alternative explanation to understand the way the different actors in the cyber security field behave, both within and between the U.S. and the EU – by quoting Johnston's words' - 'perceive the game being played' and what strategic choices they make in order to reduce the threat of cyber crime (Johnston, 1995: 63). Therefore, this research represents the first attempt to conceptualise and apply strategic culture in the EU-U.S. cyber security context, examining the various strategic actors and the role they play in influencing the transatlantic response to cybercrime.

There are several advantages in viewing the fight against cyber-crime from a strategic culture perspective. Such a study can help us to better understand the wider climate of ideas in which U.S. and EU cyber security policies operate and offer a contextualized view of the disadvantages of those policies. Similarly, it can offer us a greater understanding of the cyber cultures that are emerging within the EU and the U.S. and the way they shape the way in which both parties combat adversaries online at a detailed level. Strategic culture also helps us to understand the way in which U.S. - EU threat assessments of cyber threats from elsewhere are operating by testing their abilities to 'recognise cultural early warning signs of emerging cyber threats' (Kartchner et al., 2013: 7). Most importantly, the strategic culture approach allows us insights into the business of negotiating between the allies 'across cultures' in the field of cyber security co-operation, allowing us to identify some of the more profound obstacles to convergence and even to predict some of the implications of changing cyber security policies in the transatlantic space.

This thesis is not primarily designed to advance methodology in the realm of strategic culture, nor to engage in the somewhat arid business of theory testing. Instead it is more focused on practical policy issues, using strategic culture as a lens, it is therefore something of a moot point that strategic culture still lacks a falsifiable theory. For our purposes this is not necessary as we seek to illuminate the way decision-makers of national governments, agencies, institutions and supranational organisations like the EU comprehend cyber-threats such as cyber crime and how these understandings influence their views on cyber-crime policy (Toje, 2008: 19). In short, strategic culture is a useful interpretative lens through which to we might view transatlantic policy interaction.

Meanwhile, we can point to a strong emerging consensus that every nation has its own strategic identity, wherein decision-makers draw on a corporate memory of shared security experiences in recent history. To illustrate, if there are a series of natural disasters in the Netherlands related to extensive flooding in the last centuries, it would tackle this national security problem more efficiently due to its historical experience in the past compared to Sweden that has limited experience with disastrous floods. Moreover, it will not approach flooding as an issue for a rational actor perspective, but instead its response will be informed by collective memories of past successes and failures. Therefore, the Netherlands' past experience prompts better responses and strategies from decision makers when dealing with catastrophic floods, compared to a similar country dealing afresh with the same security situation. Learning from experience is broadly helpful, but also brings with it what Reiter calls the weight of the shadow of the past, in other words and aversion to policy options that are not the national way (Reiter 1995).

Gray explains that culture is not a 'universal therapy' for all strategic problems and therefore warns against using it as a uni-causal explanation for all sorts of policy failures or successes (Gray, 2006: 26). This research sympathises with Gray's approach to strategic culture, noting that by contrast Johnston's preference of separating culture from behaviour, while offering some operational advantages for researchers, introduces artificial separations: not unlike a doctor examining his patient's body and mind completely separately (Gray, 1999: 53). For this reason, it will be argued (drawing on Gray) that strategic culture exists 'within us; we, our institutions, our behaviour, are the context' (Gray, 1999). The purpose of this research is to apply strategic culture as a tool in order to achieve a more nuanced picture of the drivers of strategic cyber cultures by examining the problems that have arisen in EU-U.S. collaboration in the fight against cyber crime. This will help us to understand what role culture plays in development of strategies in response to cyber-crime, meanwhile illuminating other factors. Accordingly, I will present my own explanation of what we might understand by the term "strategic cyber culture". In other words, I will attempt to identify the carriers of cyber cultures both within the EU and the U.S. and demonstrate how these actors may reshape or transform collaboration in combatting cyber crime.

For the purposes of this thesis, the EU will be treated as supranational institution/union. However, it must be noted that while the U.S. is one single country built on a federal system, the EU is a unique economic and political partnership between 28 European countries that cover most of the continent. The Treaty of Lisbon (2007) abolished the three-pillar structure of the EU (European Community, Common

Foreign and Security Policy (CFSP), police and judicial cooperation in criminal matters) and made it possible to redistribute competences in three categories (exclusive, supporting and shared) between the EU and its Member States (EUROPA, 2010; Piris, 2010). Meanwhile, in the U.S. since the Constitution has taken effect in 1789, it had solely exclusive competences (the fundamental principles largely remained with some changes) (Adler, M. D., & Himma, K. E., 2009). Nevertheless, despite the fact that the U.S. is one country, there are remarkable divergences between agencies - and even within agencies that enjoy different locations. Typically, there are differences in strategic plans to guide tactical/operational cyber crime investigations between the East and West Coast. Moreover, cities like New York and states like California can sometimes appear remarkably like national actors within the E.U. These differences and lack of a unified response within the U.S. will be also taken into account when examining the fragmented U.S. approach in combatting cyber crime. This implies, that even within the U.S. - as a single country - many competing and overlapping strategic cyber cultures exist, and this helps us to explain why there is often more than one type of behaviour in response to cyber crime. Meanwhile, the institutional difference cannot be disregarded when it comes to the discussion of strategic partnership in cybercrime as every EU Member State's strategic historical experiences in the past has an impact on the way the EU collaborates with the U.S.

One of the expressions of different strategic cultures is the way in which different legal systems have been developed, partly as a result of the surge in national security law since the 1990s. If one compares the U.S. legal system with the EU system (including the different national legal systems) it is easy to see how historic circumstances and different geostrategic experiences and positions pushed them to

develop different legal environments. A critical aspect of this is the different privacy needs of these stakeholders and the need for development and collaboration in accordance with cultural norms and national legislation in two regions where privacy and personal security enjoy different philosophical and legal definitions.

It became especially clear during the interviews conducted for this project that the cultural element cannot be disregarded when one talks about any elaborate international collaboration. Until now no research has been done on cyber security collaboration from a strategic culture perspective, especially not on U.S.-EU collaboration. Certainly there are some helpful parallel materials looking at military culture, and indeed cyber culture - but not in the transatlantic context.

Logically, the next question that needs to be addressed is that of case study selection. Why have the U.S. and the EU been chosen given that cyber security is not limited only to these allies? What are the limitations of such an approach? It is immediately open to the general charge often levelled at the study of international security generally that it is not in any real sense 'international' and instead is merely an outwork of American foreign policy (Wæver, 1998). However, one might counter that cyber security is driven by technology and the US and EU are indisputably world-leading regions in this area, despite the rapid spread of mobile phone technology across regions like Africa. There would be little point in examining cyber security co-operation between Rwanda and Zaire. Moreover, while there would be a serious case for examining cyber security co-operation between say Brazil and Mexico, or indeed Russia and China who have recently signed a cyber security arms control agreement, the data for these latter countries is far from accessible. Meanwhile, by examining

U.S. - EU collaboration as a driving force in the fight against cyber-crime, we can perhaps begin to build models or opportunities for comparison with cyber security collaborations between other global players such as Brazil or India. Furthermore, it could also indicate how we might encourage greater multilateral co-operation and how to remove obstacles, cultural or otherwise.

One of the major questions that drive the operationalization of this research is how strategic culture could be best applied in the EU-U.S. cyber context? Since the thesis is based upon the assumption of complexity within large federal structures, suggesting that there is no single or monolithic strategic culture abiding in the EU and the U.S., therefore, it is suggested here that the deployment of the concept of strategic culture requires some expansion or elaboration. In other words, it need to include the various organisational sub-cultures of those agencies and bodies that act as vital players in the formation of EU-U.S. approaches in fight against cyber crime. A number of factors allow strategic culture to accommodate this flexibly.

First, one of the major strengths of strategic culture as a conceptual tool is the acknowledgement of the *importance of history* with respect to strategic behaviour (the strategic choices made by the different state and sub-state actors). Since the definition of all of the inputs of strategic culture remains a work in progress, learning from major decision mistakes that occurred in the past has been used to achieve a degree of process-tracing in order to outline the interaction between corporate memory within institutions and strategic culture, often generating a form of received wisdom. This is however problematic in the field of cyber security: while it is widely accepted that

strategic culture is historically constructed there is still not quite enough history that could help in the historical construction of strategic cyber culture.

Where does cyber culture come from in the absence of a pattern of major incidents over half a century? First, there are a range of computer-related security incidents that are analogous stretching back into the 1980s related to major defence intranets and mainframes that often fill the void. There is also some evidence of borrowing from other areas of strategic culture that present similar challenges, for example space policy and the so-called "fourth dimension of warfare". Therefore, compared to the EU, it could be argued that the 'offensive' strategic cyber culture often attributed to the U.S. military has been the result of unique 'historical developments, behaviours, and actions of the American armed services as an organisation' prompting military change. (Bisson, 2014: 5). Nonetheless, this research demonstrates that we need to be cautious of stereo-types. The military operational dimension is only one aspect of U.S. strategic cyber culture that represents an exceptional history of strategic actions. For this reason, we need a nuanced approach that avoids treating the U.S. government, or indeed the EU, as a 'monolithic' entity, especially with regard to cyber crime policy.

Second, this research acknowledges the fact that strategic culture *intersects across several disciplines* (for e.g.: psychology, sociology, political science, anthropology) and therefore, in order to conceptualise strategic culture in the cyber context various elements in numerous disciplines (for e.g.: human factor, organisational culture) cannot be disregarded. International relations scholars have tended to focus on the historical generation of strategic culture because international history is a cognate

discipline that supplies raw case study data, rather as Australia supplies iron ore to Japan. The history of crises, such as the Cuban missile crisis, has provided points of fixation, not least because issues of decision become uniquely visible in such situations. However, there are other routes to determining cyber security culture based on organisational learning that are less history-dependant (George, 1997).

Third, based on the current literature of strategic culture, behaviour and policy are mainly discussed through an elite state-centric lens that *needs to be broadened*. Especially, in the cyber context it is essential to look beyond traditional notions of the creation of strategic culture. Cyber security is a notoriously fluid field that involves sizeable private technology actors and wherein stakeholders within the state range from departments of business, diplomacy, even media and sport alongside traditional providers of security such as the police and the military. Accordingly, this research proposes that there are many strategic cultures present in the cyber security field, therefore, strategic cyber culture needs to be examined at three levels: (1) strategic/political (2) legal/regulatory and (3) operational/military dimensions. By broadening the concept of strategic culture this will facilitate a better understanding of elite decision making on cyber security policies in this complex domain.

For this reason, in the realm of cyber security at least, this dissertation takes issues with the assertions of writers such as Cornish & Edwards who still situate national security in a military space, insisting that 'without military capabilities, all talk of a strategic culture would ring hollow' (Cornish & Edwards, 2005: 802). By contrast, this study suggests that it is time to move one step beyond and, as we move into a more technical domain where ownership is at best uncertain, we confront an urgent

need to broaden the concept of strategic culture in a manner that helps to understand the way a state projects its economic and security power through a complex range of regulatory frameworks, laws, policies and strategies in order to maintain regional security 'peace', economic prosperity and the proportional allocation of resources.

To make this more explicit, the proposal of an extended, more flexible version of the definition of strategic culture is essential to this project in order to conceptualise strategic cyber culture in a way that is broader and diverse and therefore not solely limited to the context of defence and military - the traditional way strategic culture has been analysed given its birthplace in 1970s strategic studies territory of Brodie and Schelling. However, strategic culture is a two-edged sword: a better understanding of its complexities can help to overcome serious obstacles when it comes to collaboration in cyber crime but can also be the source of strategic confusion and could hinder strategic actors from certain types of decision-making unless it is rendered more flexible (Toje, 2009: 5).

When re-thinking strategic culture for the cyber domain, we need to remind ourselves that threats are not only limited to the realms of security and defence but to business and the economy as well. In other words, economic threats can be posed by climate change or cyber attacks that can damage the critical infrastructures upon which economies within the EU are highly dependent. In this way, I would argue that the "threat perceptions" of a given policy community - like the Brussels elite - would perceive a threat not only from a security but also from an economic point of view, especially in order to maintain the smooth functioning of the Single Market. For instance, the Digital Single Market Strategy is the development of a critical arm of

this. Federal organisations like the EU are also politically weak but legally strong, privileging rights and regulatory frameworks with the ECHR at its core. Therefore, developing legislation and policies against cyber threats is not just a matter of traditional security but also one of economic resilience and even rights-based identity (Checkel, 2001).

Two major challenges remain that beguile even the most flexible application of notions of strategic culture. First, it is easy to disregard the inter-play of strategic culture between government and non-government actors. The UK's National Technical Authority, GCHQ boasts less than 10% of the fundamental research budgets and staff of its largest ISP, British Telecom. Increasingly, the corporates have a global identity that does not map comfortably onto national locations. Non-government actors such as large IT giants (Google, Microsoft) have their own organisational strategic culture that the U.S. government might not have the power to control, although when it comes to the issue of cyber security the power and interests of the private sector (large stakeholders) cannot be ignored. Since the Snowden revelations of June 2013, it has proved to be increasingly important for these global giants to demonstrate their distance from national cyber security strategies and so we might reasonably expect this trend to accelerate.

Secondly, there are issues with applying the idea of cyber security culture to some of the more aggressive actors. In an era of "implausible deniability"[4] when countries like China deny even blatant intellectual property theft, we are in an uncertain space in

[4] The term refers to a condition when the subject can safely refuse to admit the knowledge of any particular truth, even though the proof is evident. It is mainly because the subject is intentionally made unaware of the said truth in order to free the subject from any responsibility associated with having knowledge about such truth.

terms of the perpetrators of cybercrime. Certainly there are some actors for which the application of the notion of strategic culture would be difficult: single adversaries such as hacktivists, violent non-state actors, criminal gangs or terrorists who play according to their own set of values and which are too fluid to lay claim even to any meaningful organisational culture. Instead, if we talk about state-sponsored attacks the concept of strategic culture could be more easily applied, but attacks are not the main focus of this project and so the problem is at best limited insofar as it is encountered here (Dvorsak, 2012).

Recent debates about strategic culture have tended to focus on the related issue of counter-terrorism, which, akin to cyber security, is a more fluid entity, displaying economic, informational and political aspects. Nevertheless, the use of force, even if unconventionally, has often been seen as the litmus test of strategic culture, betraying perhaps the strategic studies origin of the concept. Some argue that strategic culture means that 'a countries approach to the use of force has been determined by its corporate memory' (Rees & Aldrich, 2005). But we can accommodate this by thinking about the application of power, including soft power, rather than force. In essence, the type of power applied by a country or international organisation may vary across the borders. As an illustration, the power/forces that the EU prioritises in order to maintain its economic security and well-being of EU citizens can be described as soft diplomacy, rules-based system of international law, multilateralism tied together with economic benefits to maintain the Single Market resourcefully and economic resilience as an integral part of passive deterrence.

Accordingly, both the American and European strategies in this realm reflect deeply held socio-economic values and these take us back to the very meaning of culture that can incorporate any everyday activity that is symbolic of underlying ideas and shared concepts. Transatlantic differences stem from different philosophies that are 'reflected in their attitudes towards gun ownership, patriotism and capital punishment, incomes inequalities and the propensity to sacrifice social capital for material gain' (Forsberg & Herd, 2006: 27). The differences in values are present in their general foreign and security policy ideologies that Michael Smith also describes as 'warrior states' (U.S.) vs. 'trading states' (EU Member States) (Smith, 2004).

At this general level, it is widely accepted that both the Second World War and the Cold War taught different lessons to both sides of the Atlantic. The U.S. prefers to believe that the Cold War could not have been "won" without superior U.S. military power and above all the application of technical and scientific superiority in an instrumental way - whilst the Europeans tend to advocate the importance of the role of civil society and the revolutionist atmosphere present in Eastern Europe, together with a notion of third wave democratization driven by a burgeoning information revolution. Meanwhile, the lessons of the Second World War exercise a lasting impact on why the EU cannot yet act in a single voice for European security. Many political parties, notably in Denmark, Norway, the UK, France and many Eastern nations have been influenced by the Münich débacle (1938) and became firmly convinced that national independence and a resistance of large agglomerations of power is a core element in defending individual liberty (Sanders, 1999: 125). After 1945, many continental states, including Germany recoiled against the use of offensive military power. Meanwhile the rise of alliances reflects the failure of the

neutral position taken by countries such as Belgium, Denmark and the Netherlands during World War II and by Finland during the Cold War (Forsberg & Herd, 2006: 30).

Grand strategy offers us only the vaguest of way-points when considering cyber security culture. Instead, the starting point of this research is based on Marieke de Goede's hypothesis on comparing EU-U.S. approaches in counterterrorism. Counterterrorism is admittedly different to cyber security and cybercrime in that it enjoys a rather longer history and a stronger institutional memory. Nevertheless, it also has appealing similarities including its transgression of economic, political and military boundaries. De Goede's main proposition is that on the strategic/policy level it might seem that the U.S. and EU approaches to counter terrorism are very different: the U.S. is acting unilaterally by taking pre-emptive measures whilst the EU offers alternative solutions, emphasising its core values by acting as a counterbalance to pre-emptive security measures and adhering to the rule of law (De Goede, 2008: 161). In other words, Goede argues that pre-emption is often associated with the U.S. security behaviour but the fact that it is rooted in European history is often disregarded (De Goede, 2008: 163). In these complex debates, Wyn Rees counters that the divergence of EU-U.S. strategic culture can partly be accounted for in terms of raw disparities in power, arguing that 'the Europeans have expressed profound misgivings over the new American policy direction towards pre-emption', and instead regard 'terrorism as an issue for law enforcement' (Rees, 2006: 73; De Goede, 2008: 167). As a result of these strategic cultural differences the 'iciness in transatlantic relations has not been easy to thaw' (Rees & Aldrich, 2005: 914).

Remarkably, when looking at the EU policies more in depth, Goede comes to the conclusion - whilst analysing three aspects of EU counter-terror policy such as criminalising terrorist support, data retention and asset freezing – that the EU's behaviour is quite similar to the U.S. (Goede, 2008). There is an implication here that some of the European public declarations on counter-terrorism involve a degree of political posturing and even hypocrisy.

This prompts the question whether we could end up drawing similar conclusions regarding EU-U.S. behaviours and responses to cyber crime especially on the operational level? This does not mean that no differences exist on the strategic and legal levels, rather the opposite. As Bendiek argues: whilst both sides of the transatlantic share the primary principles of Internet regulation (to keep the Internet free and open, to combat crime online and to defend vital infrastructures) still, there are sharp differences on the strategic/policy and legal levels regarding how to achieve their goals (Bendiek, 2014: 1). Bendiek's proposition that the U.S. logic behind cyber security policies is driven by the military, deterrence and national security whilst the EU behaviour is rather more aligned with treating it as a police matter focusing on defence and resilience is more characteristic on the strategic level – yet there remains the possibility of convergence at the operational level (Bendiek, 2014: 2). Furthermore, it also disregards the presence of those strategic state and sub-state actors – carriers of strategic cyber cultures – that influence EU – U.S. behaviours in the fight against cyber crime. It also begs a wider question: is cyber-crime intrinsically a realm of "low politics" in which operational work-a-day co-operation is key and strategic notions are less important?

Perhaps then the very idea of an over-arching ***strategic cyber culture*** is mis-placed and instead the centre of gravity lies with a state or sub-state's self-identity towards cyber threats that has been determined by its historical experience of past cyber conflicts. Therefore, strategic cyber cultures could serve as indicators of more specific factors: what the entities – carriers of cyber cultures - identify as being in their interest in a cyber conflict/attack, what aspects of the cyber attack they recognise as a threat and what decisions they make in order to address and mitigate the cyber threat. Overall, it is suggested that historical experiences with cyber security related threats in the past could influence the codes of conduct, threat perceptions and technical developments of a state, sub-state (or non-state actor) to address cyber threats - often in conjunction with the private sector, but these are likely to rather fissiparous. Moreover, non-state actors will be increasingly important carriers of strategic cyber cultures. Accordingly, this research will give close attention to state and sub-state actors who play a vital role in countering cyber-attacks and cyber-crime on an every-day basis.

Although *regime theory* is not going to constitute a major part of the thesis, it is nevertheless worth mentioning as a cognate constructivist tool alongside strategic culture that could be used to capture the way history, ideas and culture shape relations between states or international actors. In essence, regime theory could help us to understand and predict what sorts of responses might be taken when rapid changes in the international arena occur. It attempts to clarify why states in a world of potentially anarchic interstate relations nonetheless do act judiciously by following the laws when it comes to issues such as international trade or dealing with the treatment of refugees or fighting against child pornography online (Rittberger & Mayer, 1993).

‘Regimes are institutional arrangements based upon agreed principles, norms, rules and procedures (more generally practices) which then form the model for expected and acceptable state behaviour’ (Stuart-Fox, 2004: 120). States often find themselves cooperating in regulatory regimes for the following reasons: to make sure that other states and organisations adhere to the rules and principles enshrined in countersigned international agreements which can be used by foreign policy elites as moral principles to validate their acts. In other words, regime theory recognises mutual norms and beliefs that are shared even if the foreign policy elites are coming from very different cultural traditions (Smith, 2004).

In this sense, precisely because the EU is very much an engine of regulation, it is also often labelled by academics as an international regime. Being mindful of this idea allows us to better apprehend and analyse how the norms, decision-making rules and procedures and institutions are interrelated within the EU (Krasner, 1983). In other words, Member States are forming a ‘European regime’ by fostering deeper integration and by putting emphasis on institutional joint decision-making, the implementation and application of community law, which is based on mutually accepted principles. This suggests that the ‘norms’ of behaviour that the EU represents are increasingly common and can be easily recognised like giving priority to certain acts such as compromise, negotiations, conflict resolution through peaceful terms and the appreciation of mutual benefits (Loedel, 1999: 8). Like strategic culture, these ideas could help to better conceptualise and ‘decode’ transatlantic relations in the fight against cyber crime that goes beyond the simple calculation of material power. Both offer richer approaches in international relations, embracing history and

culture in order to achieve a deeper picture of the bilateral relations between the EU and the U.S.

Stuart-Fox asserts that the way the EU and U.S. correlate to each other depends to a considerable degree on the way their leaders understand and view the world. This reflects a world of increasing summitry and presidentialism in which world leaders shape their overseas policy with increasing confidence. Their 'worldview' embraces two ideas: how the world is really established in reality and their desire to reshape it. Worldview has an impact not just on our cultural beliefs but also determines our thoughts about time and history. Our cultures and history influence the way we think about ourselves as communities or nations and how we think about others, drawing upon analogies, prejudices, stereotypes and this way shape foreign and security decision-making considerably. This implies that culture influences the field of international relations via the politics of competing for power and achieving personal goals (hierarchy, status and "face") and through national and international institutions (parliaments, parties, ministries of defence…etc.) at the highest level (Stuart-Fox, 2004: 121).

Strategic culture has been so far discussed in the current literature mainly in relation to the use of force. However, military decisions are playing a vital role only in case the peaceful terms between nations have broken down (Levy *et al*., 1995: 272). Therefore, Stuart-Fox proposes an extended conceptualisation of the framework that would include both peace and war: *foreign relations culture* and *bilateral relations regimes* (Stuart-Fox, 2004). He argues that it is essential to understand the way a nation (or supranational organisation like the EU) has developed its own foreign

relations culture with other nations throughout history, not just military and strategic but also nonviolent (peaceful) interactions such as diplomacy, cultural exchange and trade (Stuart-Fox, 2004). More precisely, *foreign relations culture* refers to presumptions embedded in a worldview in relation to which international actors or entities understand and conduct their relations with other polities. In that case we should assume that (unless there is clear evidence to the contrary) the foreign relations culture of the EU and the U.S. are different in important ways.

However, Stuart-Fox argues that it is possible to merge respective worldviews that could be conceptualised as *bilateral relations regimes* (Stuart-Fox, 2004). It refers to the shared norms, principles, required rules, expectations and procedures that are based on the mutual acceptance of two polities collaborating with each other – enable us to understand why relations between the EU and the U.S. took the form they did especially in relation to cyber crime. Both the EU and the U.S. share the same principles, values and norms on the fundamentals of Internet regulation (universal access to Internet, fight against crime and protect critical infrastructure) whereas in large part the U.S. determines these rules, but they came to be accepted by the ruling Brussels-elite as expected behaviour on both sides (Bendiek, 2014). However, there are quite a few disparities regarding their approaches and legitimate means on how to best govern cyberspace and reaching their common goals.

7. Conclusion

To conclude, this chapter reflected on the conceptual struggles and complexities when collaborating in the fight against cyber crime that can be regarded as one of the

reasons for the fragmentation of strategic cyber cultures. This chapter suggests that the theoretical implications of strategic culture discussed in the Johnston-Gray debate and through the examination of the various waves of strategic culture help to understand the way strategic cyber culture can be conceptualised. It is therefore argued that the definition of strategic culture needs to be expanded since threats emanating from cyber crime are not limited to the realms of security and defence, but extend to business and the economy as well. Therefore, the examination of transatlantic collaboration at three levels: policy, legal and operational will provide an opportunity to better understand the fragmentation and different approaches that are present and represented by different entities within the transatlantic cyber culture context.

Chapter II.

Methodology

1. Introduction - Inspiration

The issues of cyber security were highlighted during an internship at the EU Parliament during 2011. A workshop was held detailing the challenges of EU cyber security, with guest speakers Jim Lewis (programme director at the Centre for Strategic and International Studies (CSIS)) and Melissa Hathaway (former cyber security adviser to US Presidents George W. Bush and Barack Obama) who discussed the U.S. approach and how cyber security collaboration with the EU could be enhanced at the policy level. These discussions were both illuminating and exciting, constituting one of the prime inspirations for studying the challenges of EU–U.S. collaboration in the field of cyber security and examining how these challenges could be overcome in both the short and long-term.

Because my research subject is not statistically significant, even in terms of small-N, it makes sense to employ a qualitative approach. One of the most established research approaches that is used in social sciences for the close analysis of single large case studies is qualitative research deploying elite interviews. Therefore, the following section is going to explain how a qualitative method has been applied in order to understand the different strategic cyber cultures of the EU and the U.S. when they tackle cybercrime. The primary goal of this research is to understand the differences and identify the gaps in collaboration by applying a broadened definition of strategic

culture to capture transatlantic cyber-security practice and thereafter to suggest ways for improvement. This in turn involves a degree of policy-prescription.

In other words, elite interviews have allowed a granular mapping of attitudes and approaches both within and across the transatlantic relationship. The resulting analysis indicates that the concept of strategic culture that is used as the main theoretical framing for understanding the U.S.–EU mind-set in the fight against cybercrime needs to be expanded to allow us to envisage different sub-cultures operating at the policy, legal and operational levels in the field of cyber security, especially in cybercrime. In summary, the arguments underpinning this are as follows: firstly, fighting cybercrime is not limited solely to the use of force and a military level; secondly, this research demonstrates that there is more than one strategic cyber culture within both the U.S. and the EU; thirdly, it acknowledges the importance of history and that it might influence the way policymakers develop strategies to fight cybercrime, including the possibility of major shifts following perceived policy failures.

2. The definitional aspect of legal-conceptual challenges

This research also suggests that definitions matter and that how cybercrime is conceived is not a matter of mere academic debate. The U.S. has a longer history of fighting cybercrime than the EU. Despite the longer history of U.S. operations in this area, its conceptual frameworks are arguably lagging behind. As a result there are increasing differences between the cybercrime laws of the EU and the U.S., as the EU modernized its cybercrime laws in 2013, with the new Directive (2013/40/EU on

attacks against information systems) replacing the 2005 Directive (Council Framework Decision 2005/222/JHA) (Official Journal L 218, 2013). In contrast, the U.S. has not modernized the Computer Fraud and Abuse Act of 1986 (18 U.S.C. § 1030). To put it simply, the U.S. is at more of a standstill in legal developments; in contrast, the EU is more constructive. These differences in the legal dimension help us to explain why there is no universally accepted definition of cybercrime, and this is considered to be one of the fundamental challenges when gathering digital evidence in cybercrime investigations. Furthermore, whilst there have been various attempts by policy makers and scholarly studies to define cybercrime, the definitions vary, and there is still no common consensus at an international level, among policy makers or researchers, about what exactly constitutes cybercrime. Due to the complex multidimensional nature of the term cybercrime it is suggested that it is a disputable concept and therefore we are likely to see yet more competing interpretations by the different parties and therefore greater divergence in the future.

3. Research framework - Qualitative methodology

The literature discussing qualitative research methods is helpfully sophisticated and well developed (Levy, 2006; Cooper & Schindler, 2006; Walsham, 2006; Denzin & Lincoln, 2011). Qualitative data is rich in contextual information, and helps the researcher to develop their study in a more complex and iterative manner, making it ideal for the investigation of strategic culture (Silverman, 2013; Miles and Huberman, 1994; Miller *et al*, 2012). Most importantly, qualitative research starts by exploring and interpreting a situation or a phenomenon, gaining an in-depth knowledge of it, thus an understanding of the U.S. and EU viewpoints regarding cybercrime at the

strategic level can be achieved by examining the history of cybercrime and the strategies that have been developed to minimize the impact that it has on national security. Qualitative research has also been selected as an approach because it allows the exploration of new ideas and unforeseen incidences that are arising in everyday cyber security practice, since these are best captured by semi-structured interviews that allows subjects to volunteer this new information (Cooper & Schindler, 2006). Qualitative data is often gathered from interviews, focus groups and through the observation of the participants (Yunos & Ahmad, 2014). Therefore, content analysis of both written and recorded materials drawn from the interviewees' communication and comments is an essential part of the study (Cooper & Schindler, 2006).

Empirically, the focus is on the EU and U.S. contexts, specifically, exploring the contemporary challenges of EU–U.S. collaboration in tackling cybercrime at three levels (policy, legal and operational), which already suggests that the thesis is about mapping attitudes and ideas in a rapidly changing technical landscape. Therefore, an interpretive qualitative approach is proposed, since this is clearly the most appropriate way to identify the driving forces, attitudes and also to explore the mind-set of both the EU and the U.S. in relation to cybercrime. Research practice has focused on elite interviews and attending several cyber security related events and workshops. A series of internships in Brussels at the EU Parliament and in the Hague at Europol whilst conducting field research both at Georgetown University in Washington D.C. and at DG Home and DG Connect in Brussels has also permitted a degree of participant observation.

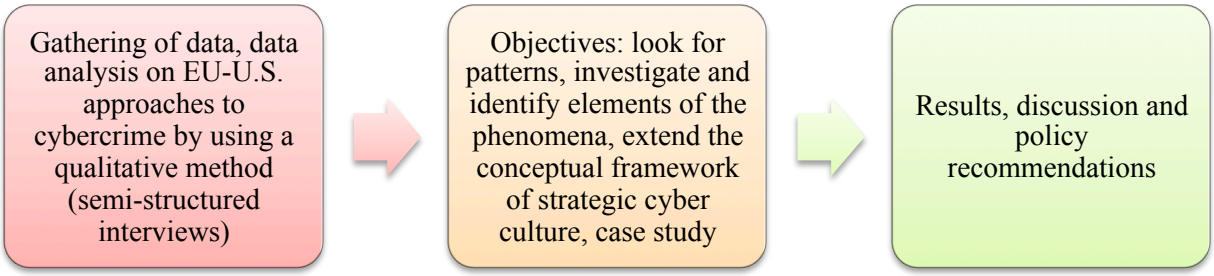
First, I was able to undertake field research as a Policy Advisor to a Member of Parliament (MEP) at the EU Parliament both in Brussels and Strasbourg from April 2013 until July 2014. Next to the drafting and advisory duties I had the opportunity to work and become familiar with a wide range of EU-related security issues through my experiences at the LIBE, SEDE, CRIM Committees. Furthermore, I was working on dossiers such as the EU Cyber Security Strategy and the Commission's proposal on the Network and Information Security (NIS) Directive that helped me to gain a deeper insight into how EU policy and decision making works in the field of cyber security.

Second, whilst conducting field research as a Visiting Researcher at Georgetown University in Washington, D.C. last summer, I had the chance to expand my network with major think tanks and also discuss my research with several experts in the cyber security field such as General Michael Hayden, former director of the CIA and the NSA.

Third, during my traineeship at the European Cybercrime Centre (EC3) at Europol in The Hague I enjoyed first-hand experience into both the strategic and operational aspects of fighting cyber crime in collaboration with the private sector. This unique experience allowed me to understand how law enforcement reaches out to various stakeholders by establishing partnerships through advisory groups (AGs) with members coming from financial services and Internet security. I was supporting and strengthening collaboration with the AG on financial services (for e.g.: Royal Bank of Scotland, Barclays, Visa Europe, UBS, ING Bank). I was also attending several public and private meetings and took regular minutes for EC3's *digital forensic laboratory*, which formed part of its ISO accreditation exercise.

Three overlapping but related techniques have been deployed to build a more three-dimensional picture.

Utilising Geertz' phrase of a 'thick description' – that is a 'meaningful description embedded in the cultural framework of the actors' – helps to understand why the local experience of individuals and different stakeholders as they seek to cooperate in cyber security related matters to our examination of culture (Merriam, 2002: 4; Geertz, 1973; Schwandt, 2007: 296). This microcosmic interpretive approach provides an understanding of the transatlantic collaboration, both from the researcher and participants' standpoints, and provides insight into the work-a-day experience of the agencies, institutions, departments and private companies' mind-sets, positions and reactions (Maxwell, 1992: 288-289; Bohman, 1991).



[Figure 2.1.]: *The framework of qualitative research methodology*

4. Interview questions

A major element of the qualitative analysis consists of interviewing a specific group of people about a topic, transcribing interviews, coding parts of the transcripts and

then linking these codes to one another (Yunos & Ahmad, 2014: 134). The semi-structured interview technique employed in this thesis commences with a few specific questions, and thereafter a more flexible structure is employed to allow the interviewee to provide further information supported by probes by the interviewer. The interview questions were provided to the individuals beforehand in order to permit a clear indication of the topic being studied. Walsham argues that, in an interpretive study, the interviews should be complemented by other forms of field data such as press, media and other publications that are related to the context of the research (Walsham, 2006).

The questions were split into two parts: a general section and a specific section. The general questions were related to the understanding and interpretation of the area of strategic cyber culture, whilst the second set of questions were related to exploring the differences and similarities of the EU–U.S. approaches in the fight against cybercrime. The questions were also phrased and refined according to who the questions were addressed to (e.g. NATO, EU Commission, U.S. Dep. of Defence, FBI, and EC3).

Samples of interview questions:

Q1. Which aspects of strategic cyber culture, in your opinion,
are most important in assessing how effective a nation or organisation can resp
ond to cyber threats?

Q2.What are the main avenues/platforms/areas of cooperation with regard to cybercrime between the EU-US?

Q3.How do you think the main challenges to cooperation can be addressed in t
he short/medium/long term with regard to cyber security (broadly) and
cybercrime (specifically)?

5. Data collection - Semi structured interviews

As we have already indicated, when selecting a suitable method for primary data collection, semi-structured interviews were chosen for the interviews with policy makers, law enforcement officials, politicians, representatives from the private sector such as the EU Commission, the US Department of Homeland Security (DHS), the US Department of Justice (DoJ) and Europol in order to develop a fresh analysis on an under-researched area by allowing the subject to volunteer new data. It was also important to establish the perspectives of state agencies related to the approach taken when preventing or managing cybercrime-related risks. At the strategic level, wider government policy may also be expressed in a secondary format such as reports by agencies tasked with investigations, or else in internal documents compiled by particular departments outlining strategies that have been, or will be, pursued. Examples include the *EU NIS Directive* (2016), *EU Cyber Security Strategy* (2013a), *DoD Cyber Strategy* (2015), and *International Strategy for Cyberspace* (2011). One of the fascinating aspects revealed by this research is the fundamental underlying conflict between these formal statements and attitudes revealed in everyday operations, which is suggestive of important differences in the balance of real power between states and sub-state actors.

The effectiveness of interviews is largely dependent on the communication and interpersonal skills of the interviewer (Clough & Nutbrown, 2012; Ritchie *et al*, 2003). These skills are essential in order to establish trust and to demonstrate understanding towards the participant, thus creating a comfortable atmosphere in which the interviewee is encouraged to speak easily and freely (Newton, 2010: 1).

Newton identifies two types of interviews: "structured", which have clear outlines supplemented with questionnaires and "unstructured", which place more emphasis on observation (Newton, 2010: 1). Conducting interviews played a vital role in this research as it not only assisted with the collection of rich data, but observation of the interviewees' language and contextual-relational aspects provided an understanding of their personal perceptions, values and beliefs related to the approaches used by government, institutions and agencies in the fight against cybercrime. Both in the EU and the U.S, interviews also helped this research to reach out beyond information gained solely from strategic, policy and legal documents by providing an "out-of-box experience", in other words, by offering a first-hand insight into the personal views of the participants on that matter, and this was especially important in attempting to map something as elusive as strategic culture. Moreover, since cybercrime-related issues are fast evolving, official policy documents often do not reflect accurately how collaboration is conducted operationally and might also miss out important aspects of informal modes of collaboration.

The central question that drives this thesis is the impact that strategic culture has on the EU–U.S. collaboration in the fight against cybercrime, and that requires a greater understanding of the thoughts, behaviours and roles that state and sub-state actors play when collaborating with each other to suppress cybercrime at the strategic, legal and operational levels. These research interviews also provide the opportunity to compare the similarities and differences in the attitudes of EU–U.S. entities when dealing with cyber security, to identify what factors influence their behaviours, to establish how their relationship has been evolving over time and to identify the important changes that have resulted in improved collaboration. In essence, the aim of

the interviews is two-fold: not only to gain descriptive accounts of the interviewees' standpoints regarding a particular activity of the transatlantic cyber security collaboration, but also to expand the concept of strategic culture within the cyber context. More precisely, strategic culture as an analytical tool is particularly suitable for this research, allowing us to better understand the foundations of strategic behaviour and the decision-making procedures of EU–U.S. security communities concerning the threat presented by cybercrime.

The most important methodology this thesis relies on for data collection is semi-structured interviews with selected cyber security officials, former officials, law enforcement agents and cyber consultants from the private sector. According to Bryman, semi-structured interviews appear to be dominant when qualitative research is conducted (Bryman, 2006). However, in this case, the thesis has avoided a single method of data collection, it has been adapted as the interviewees were consulted for further explanation and interpretation on multiple occasions. Additionally, data was also collected in forums, through participant observation and then, at a later stage, all this was also compared to relevant documents. In short, the limitations of semi-structured interviews were mitigated.

Nevertheless, semi-structured interviews offer greater flexibility as they can follow either a general interview type guided approach or a conversational approach. At the outset at least, this thesis followed a general interview guided approach where an interview guide listing the interview questions and issues that need to be covered is provided to each interviewee. This allows similar information to be gathered, and, according to Valenzuela and Shrivastava, is a more focused approach (Valenzuela and

Shrivastava, 2008). The interviews were recorded after approval and were also transcribed and coded in order to compare the differences in attitudes, behaviour and perceptions of several actors that play a key role in the EU–U.S. collaboration in the fight against cybercrime.

This thesis made use of an extensive array of informational sources and was built upon 86 interviews and 39 cyber security related conferences/ workshops/meetings attended in the U.S. (Washington, D.C), Belgium (Brussels, Leuven), the UK (London, Oxford, Warwick), the Netherlands (the Hague) and Hungary (Budapest) between 2012 and 2016. Depending on the circumstances, interviews were carried out either face to face or through the use of online software such as Skype.

The interviews were conducted with current and former government officials, politicians, military personnel, corporate executives and employees, law enforcement officials who directly deal with cyber security operations or policies, and also with professors and researchers from academia. More precisely officials from the European Cybercrime Centre (EC3), J-CAT, FBI, USSS, DHS, DoD, DoJ, UK National Crime Agency (NCA), ECTEG, NATO, Eurojust, DG HOME, DG CONNECT, EU Parliament, EEAS, CEPOL and private sector representatives from Symantec, Microsoft, Facebook were interviewed.

Reaching out to all the different stakeholders who work in the field of cyber security seemed to be the best approach to gain a clear understanding of the challenges of collaboration between public-public and public-private partnerships on various levels.

However, it is also essential to recognise the inherent weaknesses when conducting semi-structured interviews. As Denscombe highlights, the participant's responses during an interview, and the extent to which the participant is willing to share and reveal information honestly, is often dependent upon their impression of the interviewer (Denscombe, 2007: 184). The problem can be exacerbated by the nature of the topic of discussion as it could make the interviewee cautious about what answers they provide, and cause them to be selective according to what they think is required in the situation (Gomm, 2004). Therefore, it is essential to state clearly the purpose and topics of discussion right at the beginning of the interview as this helps the interviewee to feel more comfortable. Furthermore, it is sometimes challenging to capture the exact position of the interviewee on this topic, since the goal of the interviews was also to help determine whether the attitudes to collaboration are driven by cultural, institutional or personal forces and these are intrinsically nuanced, even elusive subjects.

6. Ethical concerns

Semi-structured interviews provide the participant with the freedom to express their private thoughts and feelings, but establishing a trusted relationship is largely dependent on the social and communicational skills of the interviewer (Newton, 2010: 6). From an ethical point of view despite these qualities being beneficial, ethically they are very sensitive (Newton, 2010: 6). Therefore, it is essential to review confidentiality issues, anonymity in certain cases, and the questions that it is intended to discuss. All aspects of the thesis have been conducted in full compliance with the frameworks set out by the ESRC and the Warwick University ethics committee.

7. Limitations

Finally, there are some limitations to the thesis that should be underlined:

Firstly, since the focus is mainly on the U.S. and the EU context, it inevitably excludes the different ways cybercrime has been combatted in other parts of the world such as the Middle East and Asia. We know very little about cybersecurity across the global south.

Second, due to the contemporary nature of this topic, and as a result of rapid developments in the field of cyber security, news sources have often been used to map very recent developments, or elusive issues, but these might lack accuracy and authenticity.

The third limitation relates to the "secret" nature of cyber security. The majority of the information on threats and capabilities remains classified and is not available in the public domain. This is partially due to the competition among the different stakeholders in the cyber security domain. Therefore, national security imperatives mean that it is difficult to grasp all the elements and gain a comprehensive picture of the transatlantic cyber domain.

Chapter III.

EU strategic cyber culture

'Software of the machines may be globalized, but the software of the minds that use them is not.'
(Hofstede)

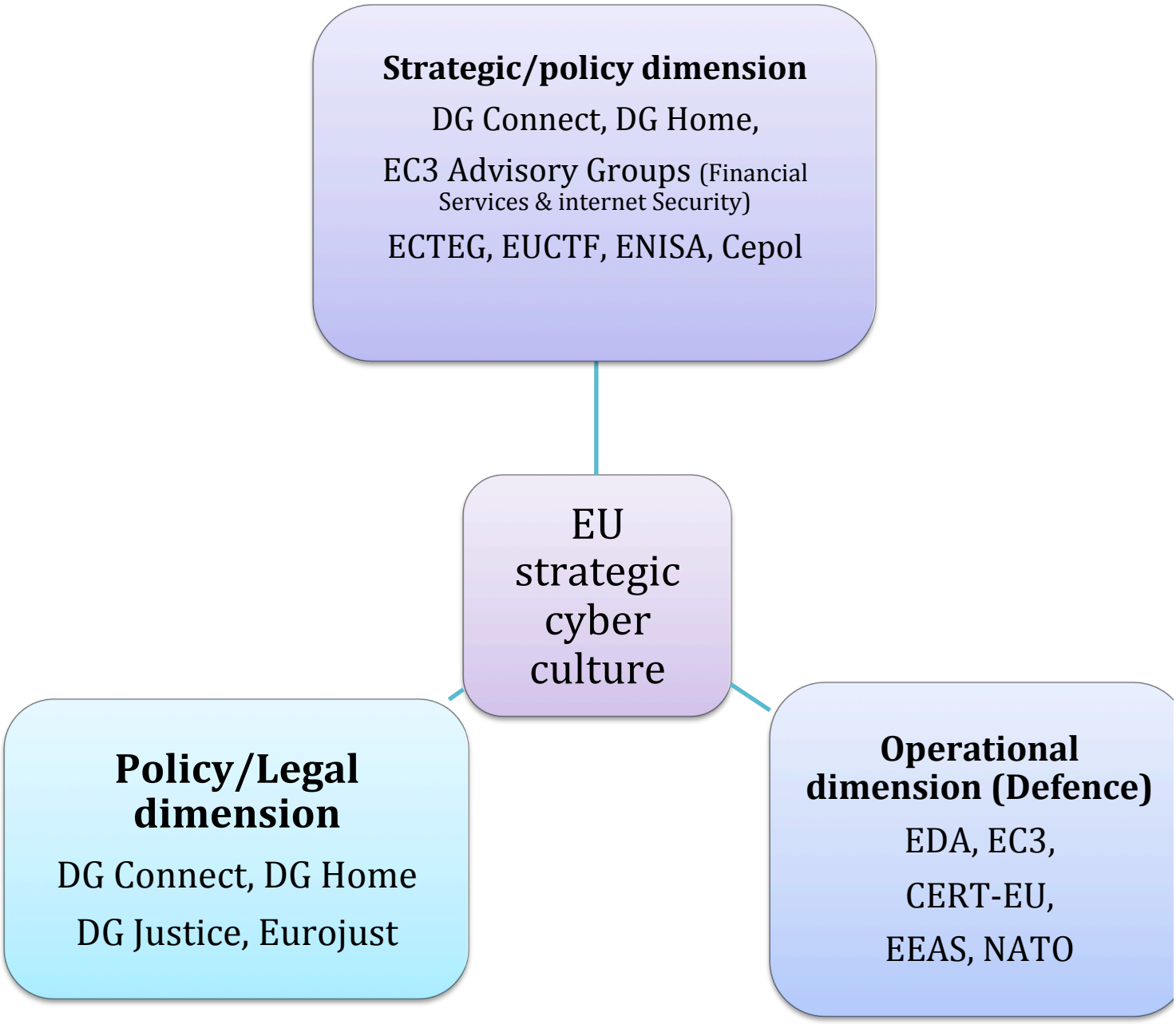
The European Union (EU) consists of 28 different Member States and each one carries its own distinctive historical baggage of strategic decisions. This chapter will provide evidence that there is more than a single overarching strategic culture at the EU level. Furthermore, it will build upon the assumption that the concept of strategic culture could be used as an investigative tool to assist with an understanding of the various approaches/attitudes to cyber security (broadly) and cyber crime (specifically) as driven by the Brussels elite at both the strategic/legal and operational levels.

The theoretical work carried out by Toje provides several important insights that assist in understanding why the application of strategic culture provides analytical traction in the context of EU cyber security policy: (1) the concept is vigorous and adaptive; (2) it distinguishes between words and actions in a way that helps to examine the outcomes of the European Council, the Commission, the European Cybercrime Centre (EC3) and informal groupings such as the Network and Information Security (NIS) Platform; (3) it is not restricted solely to one type of strategic culture and allows us to take account of others that coexist within the various nation states, the EU agencies (for example, ENISA, EC3), the EU institutions (for example, DG Home), NATO and the EU as a supranational organisation (Toje, 2008: 9). In addition, strategic culture can be applied not just at the state level within a national security context but also at the institutional level - the term organisational

culture, or even *institutional culture*, is often used (Katzenstein, 1996; Powel & DiMaggio, 1991; Biava et al. 2011: 1230).

This chapter draws on the fieldwork carried out among European civil servants and politicians in Brussels between 2013 and 2014. It explores the way in which the EU elite have attempted to advance an EU cyber security policy by diffusing their vision of 'European consciousness' and 'European strategic cyber culture' among the peoples of Europe and international partners such as the U.S. This chapter will also therefore seek to identify and examine the key actors who are shaping this strategic culture and who have been the drivers in disseminating this vision.

This chapter will begin by examining the traditional view of EU strategic culture through the development of the Common Security and Defence Policy (CSDP) and its relationship with cyber defence. It will be argued that, in order to understand and analyse the EU's approaches to cybercrime, the concept of EU strategic culture should be expanded to include the legal, strategic/policy and operational dimensions and should not be narrowly limited to the way a nation uses force (see Figure 3.1). Therefore, a more comprehensive, perhaps even more "European" understanding of strategic culture will be proposed. This will help to build on the section that explains the different institutional contexts within which cyber security operates in the EU and what this means for strategic cyber culture broadly and, more specifically, in relation to cyber crime.

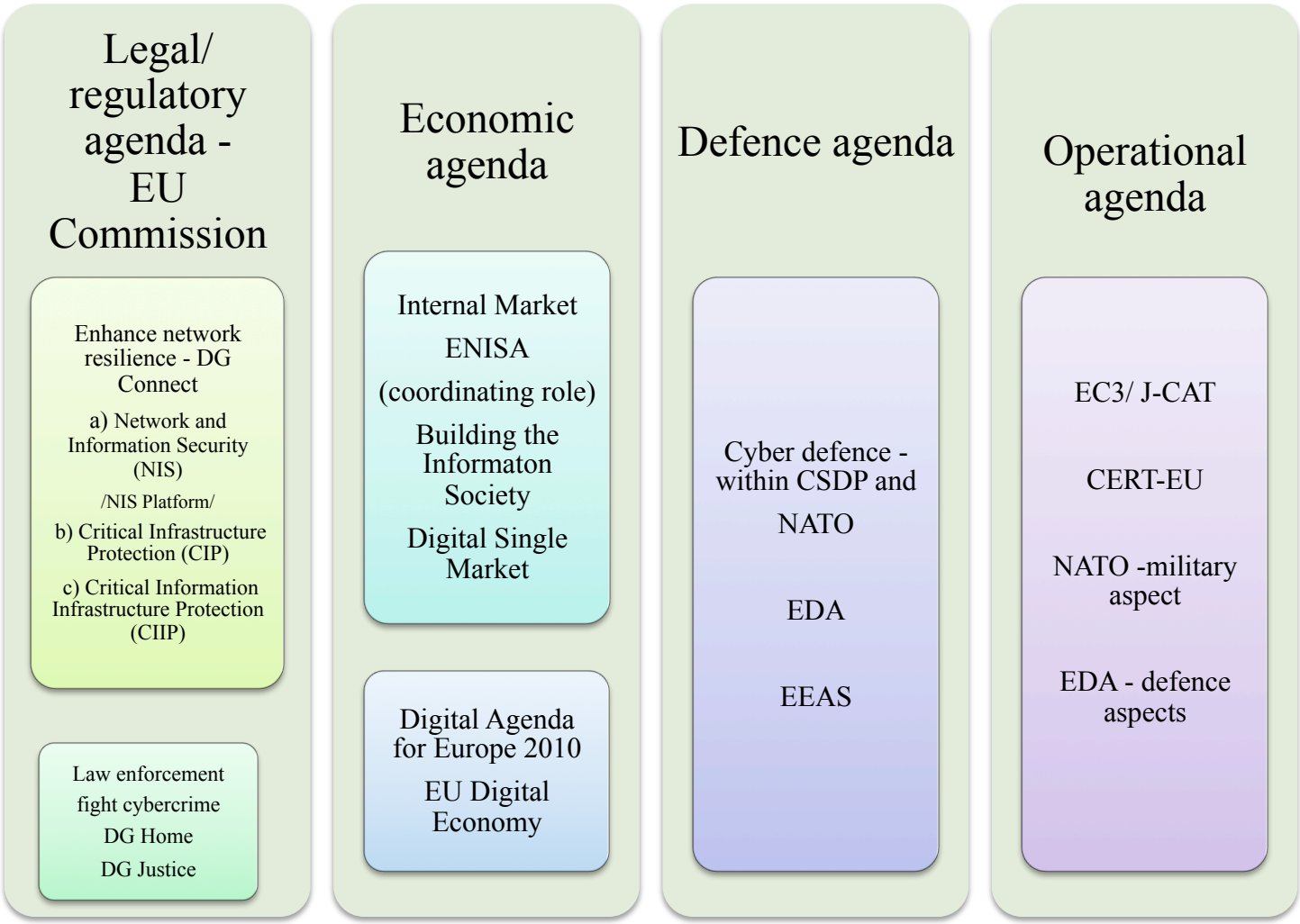


[Figure 3.1.]: *Pillars of EU strategic cyber culture*[5]

What makes the issue of EU cyber security unique and fascinating is that it connects a range of important sectors that fall within the wider ambit of new security. First and foremost, the smooth running and growth of the EU digital economy is hugely

[5] Note, this illustration serves as a heuristic device since EU strategic cyber culture does not separate quite as neatly in practice as there are many overlaps between the various levels.

dependent on critical infrastructures (CIs) and Information and Communication Technologies (ICTs), therefore any disruption to these capabilities may have disastrous consequences for the governments and the social well-being of EU Member States. Secondly, in the fight against cybercrime, the EU institutional pillar's structure is driven by DG Home and DG Justice which are the major players in the prosecution of cybercrime, whilst other elements, such as enhancing the network resilience, fall under the competences of DG Connect. Finally, cyber defence is overseen by the European Defence Agency (EDA), while the EU External Action Service (EEAS), the European Cybercrime Centre (EC3), the European Network and Information Security Agency (ENISA) and the European Union Computer Emergency Response Team (CERT-EU) are responsible for both the operational and technical level of EU cyber security. Accordingly, both the EU's approach to cyber security generally and cybercrime specifically is remarkably fragmented within its pillar structure (see Figure 3.2).



[Figure 3.2.]: *The EU's fragmented approach to cyber security*

Nevertheless, the capacities in the areas of Justice and the Single Market play a vital role in the establishment of EU wide cyber security measures, as they are applicable to e-crime and IP theft. Consequently, one might assume that the EU cyber security standards will be extended to states that are influenced by the rules of the Single Market. An example here is the case of Norway. As frequently predicted by adherents of regime theory, this "extraterritoriality" will have a valuable influence through the export of EU cyber-security measures and the extension of improved standards and conventions beyond the boundaries of the EU.

First, the chapter will begin the discussion by exploring what might cause the fragmentation of EU strategic culture. The following sections will move on to the development of the CSDP, the EU's related threat perceptions and the influence this has had on EU strategic culture. Gaining a clearer picture of the transformation of EU strategic culture will provide an understanding of the development of strategic cyber culture within the EU, the driving forces behind the EU cyber security policy and the EU's approaches to cybercrime. In order to understand the non-static nature of strategic cyber culture at the EU collaborative level this chapter will suggest a linkage between CSDP and cyber defence as a starting point for exploration. Then the chapter will progress to demonstrating the decentralised approaches that exist at the EU level by examining the policy, legal and operational dimensions of strategic cyber culture.

1. Fragmented EU strategic culture

Before embarking on a general examination of the various driving factors of EU strategic cyber culture and the more specific focus on cybercrime, it is worth examining the contrasting attitudes held by scholars when debating the existence and nature of an EU strategic culture. From a cultural context point of view, one of the main arguments against the presence of a common EU strategic culture has been that the EU still conducts many of its operations in a national rather a supranational environment (Hadfield, 2007: 61). According to Kaelberer, European identity is still weaker than the national identities and the only real substance lies in its institutional and instrumental setting (Kaelberer, 2004: 172). Nevertheless, he admits that common practices constitute an invisible bond among Member States, arguing that:

> … the cultural tradition of antiquity, feudalism and the uniformity of the medieval period, the experience of the Reformation, Renaissance, Enlightenment, nation state formation and the industrial revolution are all

> common experiences of Western Europe beyond individual nation states (Kaelberer, 2004: 173).

Nevertheless, divergent national tendencies originating from short-term interests or historical pasts are still posing an obstacle for the EU as it seeks to speak with a single voice. Others, like Hampton, refer to the 'oasis' metaphor: whilst there is the emergence of an EU security culture, considered by many as an 'oasis', the diverse geopolitical assumptions and perspectives about threats and security that exist within each Member State make it difficult for a pre-eminent EU strategic culture to materialise (Hampton, 2013). Therefore, Hampton argues that EU strategic culture remains more of a mirage, whereas national strategic cultures continue as both the dominant and primary challenges in the development of a coherent EU strategic culture (Hampton, 2013: 52).

This research supports Hampton's analysis, suggesting that that there is certainly no single and pre-eminent EU strategic culture. This fact became apparent in the 1990s when attempts were made to produce the White Paper on Defence by merging the different EU strategic cultures into one. This stalled and serious competences in defence remain to be developed. In other words, for the EU, military power still remains a secondary issue and instead it puts greater emphasis on economic power (Rees, 2011: 32). Thus, the legal and regulatory culture, rather than the military and security dimension remains the EU's primary source of power, and this has intriguing implications for cyber security and cybercrime as they cross all these domains.

1.1. *Ambiguous definitions of EU strategic culture*

Other distinguished scholars, notably Toje (2008), Meyer (2006), Norheim-Martinsen (2011), and Cornish and Edwards (2005) suggest with some confidence that EU strategic culture has in fact developed during the existence of the Union, shaped by its geopolitical environment, history, capabilities and shared values, as well as the convergent approaches of its political leaders. Although the authors have individual arguments that differ in the detail they broadly concur and propose the following main characteristics of EU strategic identity:

- Maintenance of regional security and good Neighbourhood Policy
- Representing strong economic power vs. weak military and political influence
- Advocating multilateralism, normativeness, secularisation, rule of law and consensus over actions that can be hindered by differences in national strategic cultures
- Reliance on the U.S. in issues of governance and military support through NATO
- Sustained legitimacy
- Application of European codes of conduct: using force only in an act of self-defence
- Promotion of shared norms, values and best practices
- Event-driven approach, sometimes resulting in ad-hoc decisions
- Focus on projecting soft power tools while prioritising economic interests
- Absence of financial, decision-making capacity and 'political will' to develop hard military power outside of NATO
- Pre-emptive actions through diplomatic and economic pressure

(Borrowed and updated from Toje, 2009: 18; Bendiek, 2014 and Forsberg & Herd 2006: 6)

In order to examine the relationship between EU strategic culture as comprehended by these scholars and its precise relationship to the development of EU cyber security, it is essential to provide a definition of EU strategic culture. Most of the definitions

are still quite broad, but nevertheless there are some clear concepts and attitudes to strategy, or perhaps more accurately, to statecraft which are distinctly European. A review of the classifications by Gray (1981, 1999, 2006), Johnston (1995, 1996), Norheim-Martinsen (2011), Longhurst (2004), Meyer (2006) and Cornish and Edwards (2005) identify the following indicators in terms of the fundamental and historical conceptions of security which may be used:

(1)

> Strategic culture is referring to modes of thought and action with respect to force, which derives from perception of the national historical experience, from aspirations for responsible behaviour in national terms (Gray, 1981: 22).

(2)

> Strategic culture is comprising the socially transmitted, identity-derived norms, ideas and patterns of behaviour that are shared among a broad majority of actors and social groups within a given security community, which help to shape a ranked set of options for a community's pursuit of security and defence goals (Meyer, 2006: 20).

(3)

> In that sense, acting militarily, but well within the overarching conflict-preventive (read: more benign) parameters, has become an end in itself and a way to legitimize military force as an inherent and natural part of an EU strategic culture (Norheim-Martinsen, 2011: 526).

(4)

> … the political and institutional confidence and processes to manage and deploy military force, coupled with external recognition of the EU as a legitimate actor in the military sphere (Cornish & Edwards, 2005: 802).

From these four definitions it is possible to observe an emerging consensus that strategic culture is deeply 'embodied' in the wider security context; therefore, an alternative approach is suggested. If it is accepted that the definition of strategic culture for the EU should not be restricted to narrow strategy, but should instead be expanded to include aspects of economy, technology, geography, the rule of law, and

indeed, the institutional character of the EU, then the starting point in a security context might be regarded as the 'keystone' of the EU, namely the Treaty of Rome signed in 1957 which established the European Economic Community (EEC) - the internal market (Dvorsak, 2012). It is also important to remember that the political union of the EU lasts only as long as the functioning of the Single Market and security of this is at its core.

1.2. EU strategic culture through 'traditional' lenses

In terms of a wider security culture, Europe has been influenced by several factors: (1) different historic experiences in war, (2) the evolution of a post-national identity in the geopolitical environment in the aftermath of the Second World War and (3) the downfall of European religiosity in the 1960s (Hampton, 2013: 53). Importantly, Peter Berger proposes the idea of *European exceptionalism* regarding the issue of religion, arguing that in Europe secularisation and de-religiosity have become central both in cultural and political terms (Berger, 1999: 12-14). This is a broad trend across the EU, albeit it more advanced in Western Europe than in recent additions from the East.

Yet there are also marked national differences, and the UK, for example, continues to preserve its unique national identity and consistently claims a distinctive 'way in warfare'. These different experiences (especially in war) and divergent attitudes to the use of military power, for example, the British and German perspectives, underpin the lack of the presence of a strong and central military culture. The interviews conducted in Washington DC indicated that there is also an abiding assumption that the EU is lacking a unitary voice and therefore there is still the problem of "who to call" when

there is a security concern in Washington. This challenge is also present when establishing cyber security collaboration on the strategic/policy level. For this reason the U.S. often prioritises bilateral relations over multilateral negotiations in order, as one U.S. government official remarked, simply "to get things done". North Atlantic Treaty Organization (NATO), alongside other agencies such as Europol and high-level strategic and operational platforms, such as the EU–U.S. working groups and Joint Investigation Teams respectively, always remain another option as a vehicle of U.S. and EU collaboration. On the one hand, NATO is an attractive vehicle for it extends the U.S. security umbrella relating to the collective self-defence of its members' territories, which was reinforced under Article V. On the other hand, one might argue that the EU lacks a military aspect to its security culture precisely due to the division of labour between NATO and the EU. The same division of labour is applicable to EU cyber security: whilst NATO deals with the military aspects; the EU is in charge of the civilian aspects of cyber security.

James J. Sheehan, one of NATO's more eminent and experienced officials, claims that these profound societal changes have had a direct impact on European views of fighting wars. For instance, without overt religiosity, a strong sense of expansionist nationalism or indeed neo-conservative 'muscular liberalism' it is difficult to find another tool to be used in order to justify *jus ad bellum,* 'the right to war'. During the Second World War, Christian churches in Europe, even in Communist Russia, played a vital role in mobilising the masses to fight against the 'evil' that was manifested in Nazism and totalitarian ideologies (Coupland, 2006: 6). But, as a result of the negative reverberations of that conflict, European security culture has become demilitarised, in other words, Europeans have rejected fighting wars and indeed

'violence itself became delegitimised' (Sheehan, 2009: 109). According to Hampton the transition from national to *cosmopolitan exceptionalism* naturally brought different approaches to handling security threats. The consideration of an existential evil threat progressed to a notion of "risks" as problematic issues that must be controlled through regulation (Hampton, 2013: 54). As a consequence, for the majority of Europeans, 'evil' is not a driving force in external policy and such ideational appeals in foreign policy have lost any underpinning religious meaning. However, while the 2007 EU Constitution excluded the legacy of Christianity, this does not mean that the role of religion as a cultural unifier has completely disappeared from Europe (Hampton, 2013).

During the late colonial era both Britain and France aimed to preserve their position in world affairs and their permanent seat on the UN Security Council by advocating technologically advanced and flexible military force throughout Europe (Meyer, 2006: 1). This ambition is still present today and can be observed when examining the European geopolitical situation more closely. In terms of willingness to deploy military force, Britain and France undoubtedly remain the most active members. This can be explained, in part, in terms of the historical legacy of post-imperial responsibility that has drawn Britain into Sierra Leone, or drawn France into various episodes in Syria and the Lebanon in recent decades. However, the aftermath of the Second World War taught European nations different lessons, which impacted on four vital areas:

- Strong economic culture and commercial ties can guarantee collective security (nations with strong business ties are less likely to go to war against each other)

- Institutional culture serves the basis of EU legal/regulatory principles

- Cultural normative agenda promotes EU values through civilian soft power tools

- Security and defence policy is based on the United Nation's (UN) approach with a focus on symbolism, foreign aid and legitimised actions.

Drawn from (Schmidt & Zyla, 2013: 9)

[Table 3.1.]: *Drivers and obstacles of EU strategic culture*

EU strategic culture (EU SC)	
Drivers	*Obstacles*
- Multilateral and internationally legitimatised approach to threats - Identification of new threats and the continuing adjustment of EU institutional capabilities to tackle threats - Political consensus among Member States to launch and manage *CSDP operations* - Operational practice and institutional evolution - Lessons learnt from the operations - Military and civilian participation at CSDP missions *Strategic documents with guidelines shaping EU SC:* - EU Global Strategy 2015 - Framework of European Security Strategy (ESS) of 2003 - Report on its Implementation 2008 - Internal Security Strategy 2010 - Key documents within CSDP (Somalia, Congo, Chad) *Institutions that embody EU SC:* - Political and Security Committee (PSC) - European Security and Defence	- Not a state but a hybrid entity - Complex multilevel-governance - Lack of European models within the organisation of defence that could foster convergence - No agreement regarding the methods and end goals of security and defence policy - Divergent military doctrines and traditions - Enlargement of EU membership increases divergences - Different historical experiences and collective memories - Internal tensions within national strategic cultures - Small and medium states are reluctant to maintain full spectrum of defence and are rather looking for collective solutions - Difficulty of mobilisation of weaponry and logistics at short notice - No integrated command structure

College (ESDC) - European Police College (CEPOL) - European Defence Agency (EDA) - EU's Institute of Strategic Studies in Paris - EU military committee (EUMC)	

Adapted and updated to December 2014 from Biava et al. (2011, Table 1. pp. 1231)

Some analysts maintain that the presence of deep strategic-cultural divisions among Member States poses an insuperable obstacle to the development of a common strategic culture. Others argue that the nature of the Union simply allows the luxury of division, since it is *not* a nation-state/country and does not need to express its purposes with a singular voice (Larivé, 2014: 131; Biava et al, 2011; Meyer; 2006). According to Cardoso, three different security sub-groups can be distinguished among the EU Member States:

1. *Pro-U.S. or Atlanticists* (UK, the Netherlands, Central and Eastern European Countries) vs *Europeanists* (France, Belgium, Germany and Finland)
2. *Multilateralists* (most EU Member States) vs. *sovereignists* (UK) and *neutralists* (Austria, Ireland)
3. *Those in favour of applying the use of force* (former colonial powers such as the UK and France) vs *pacifists* (Germany, Nordic countries)
   (Cardoso, 2009)

From the point of view of strategic culture, Italy maintains a position that differs from both the great powers and small states. Whilst Italy maintains multilateral relations within NATO, the United Nations (UN) and the EU, it also emphasises bilateral relations with the U.S. and still regards them as their main ally in defence and security issues (Marrone and Di Camillo, 2013: 193). As Italy also maintains some post-imperial ambitions in the Mediterranean and the Middle East, Italy could be classified into both the Atlanticists and Multilateralists groups.

Howorth, by contrast, argues that there are seven divergences across the national strategic cultures of EU Member States that can be determined according to their approaches to war, peace and security:

(1) *Allies* (Germany, Denmark) vs *neutral/non-aligned* (Sweden, Finland, Austria, Ireland)
(2) *Atlanticist* (Netherlands, Portugal, Denmark) vs *Euro-Atlanticist* (Belgium, Luxembourg, Spain, Italian defence ministry, Ireland, Finland) vs *Europeanist* (UK, France, Germany, Greece, Italian foreign ministry)
(3) *Nuclear* (UK, France) vs *non-nuclear*
(4) *Preferring power projection* vs *territorial defence*
(5) *Pro-military* vs *pro-civilian* (Nordic states)
(6) *Large* vs *small states*
(7) *Weapons system providers* vs *consumers*

(Howorth, 2002; Biava et al., 2011)

1.3. The effects of strategic cultures on EU policies and legislation

It is necessary to examine 'How else to explain Germany's reluctance to send troops abroad, Poland's difficulties with trusting European partners, Britain's attachment to the U.S., France's insistence on a global autonomous role?' (Meyer, 2005: 51; Lantis, 2002). Germany, for instance, is notably cautious about engaging in military action because of its historical involvement in the Second World War. Its brutal aggression resulted in a strategic defeat, extensive casualties and moral shame, and this imparted an indelible lesson, resulting in the development of *civilian power* as the cornerstone of German foreign and security policy (Harnisch and Maull, 2001: 1). This has also made Germans sensitive to the dissemination of any propaganda or radical movements. This also extends into cyber policy as Germany is also a strong advocate of a free and open internet and is against any censorship of illegal content online. This can be explained not only by a revulsion of the wartime Gestapo but also by the

German Democratic Republic or GDR's (informally known as East Germany) unique experience with the STASI, their official state security service that employed 500,000 secret informers to listen to the citizens' phone calls (Fischer, 2010).

In contrast, not long after CISA – the U.S. surveillance bill, the 'Cyber Security Information Sharing Act' – passed through the Senate, France ratified its own controversial surveillance law called the "*Proposition de loi relative aux mesures de surveillance des communications électroniques internationals*", that according to *Access Press Release* is 'very invasive and has little oversight built in, so its power – and potential for abuse – is great' (Access Press, 2015). Despite the fact that France has been regarded as a bulwark of liberty throughout history, in the wake of the terrorist attacks, France has moved rapidly toward draconian security measures. Since December 2014 four laws that all grant greater surveillance powers have been passed – the Anti-terrorism Law, the Military Programming Law, the Intelligence Law and the International Surveillance Law (Massé, 2015a).

One of the greatest concerns of privacy advocates regarding the surveillance bill is that a sunset clause in the intelligence law (aka French Patriot Act) is lacking and, compared to Germany, there is a lack of independent oversight or judicial control, which in effect furnishes the Executive branch, especially the Prime Minister with extensive power (Massé, 2015b). This concern over the extensive use of digital surveillance was also highlighted by Dinah PoKempner, Human Rights Watch (HRW) general counsel, who argues: 'Though the goal of the bill is to place France's surveillance practices under the rule of law, it in fact used to clothe a naked expansion of surveillance powers,' (HRW, April 2015).

Accordingly, as Meyer states, historical experiences, 'traumatic defeats, oppression, betrayal and exclusion, guilt as well as military triumphs plant themselves deep into collective memories as "lessons learnt" and "beliefs held"' impact on Member States' current approaches to security and defence issues (Meyer, 2005: 51). For instance, Finland puts emphasis on homeland security through national conscription, whereas both UK and France, conversely, have a colonial approach towards the use of force, despite the UK possessing an Atlanticist orientation, while the French have a more European affiliation (Biava *et al*., 2011: 1232). As a consequence, the more states that join the EU, the wider this divergence becomes.

Internal tensions or divisions are also present within national strategic cultures and these too pose an obstacle to regional convergence. According to Dalgaard-Nielsen, the reason for Germany's reluctance to join the Iraq invasion was not just because of an anti-American attitude but also because of 'the co-occurrence of two competing schools of thought within Germany's strategic culture' (Dalgaard-Nielsen, 2005). Another similar example is Denmark, where Rasmussen states that two strategic cultures are present: *cosmopolitanism* that advocates neutrality, non-militarism, and international organisations, and *defencism* that favours alliance with NATO and military readiness (Rasmussen, 2005).

1.4. Influencers of EU strategic cyber culture

A nation's corporate memory, broadly speaking, refers to the memory that has been acquired over decades, or sometimes centuries, relating to the manner in which a nation has led wars, diplomacy foreign and security policies. Logically, corporate memory could also be used as a starting point when examining cyber policy. The EU

experience with cyber policy is, however, extremely short compared to the U.S. Some critics might therefore say that, due to the EU's limited experience, in other words, their shallow 'corporate memories' with regard to cyber attacks, most EU Member States could not develop their own culture proportionate cyber policy. Nevertheless, despite the fact that the EU only came up with its cyber security strategy in 2013, which was quite late compared to the U.S., some of the leading EU Member States (MS) had already experienced and developed an approach and culture towards cyber security due to their extended experiences with cyber threats.

The differences in attitudes toward and experiences of cyber security among Member States have created fragmentation in the development of a cohesive single EU strategic cyber culture. This thesis therefore suggests that considering the EU as having only a single strategic cyber culture should be avoided. As a result of the fragmentation, some of the more advanced Member States have become more influential in shaping the EU's approach to cyber security; in other words, the EU cyber culture. Effectively, this suggests that their behaviours and responses towards cyber threats cannot be ignored.

When studying EU strategic cyber culture, it is important to take into consideration different angles represented by the "carriers" of cyber culture. Looking at it from only one perspective (for example, from the UK or German point of view) might create a risk of providing a vague and one-sided analysis. To repeat, since EU cyber culture constitutes all 28 EU Member States, it would be difficult to talk about only one cyber culture, and due to fragmentation many cyber cultures are present within the EU. The following section will examine individually some of the more advanced Member

States, specifically Estonia, Germany, France, and the UK, who could arguably be considered as the main influencers shaping EU regulation, law and the operational strands of strategic cyber culture. Field research carried out in Brussels indicated that these Member States have a greater influence and play a more pivotal role in regard to EU cyber security issues than other Member States do. Examining their behaviours and cyber cultures could provide a better understanding of how they have influenced and shaped the EU approach to cyber security and, subsequently, how this has effected the EU–U.S. collaboration in cybercrime.

Estonia:

It might be argued that Estonia is the only EU Member State with a highly advanced cyber security culture. This was developed in the wake of a remarkable cyber event in 2007, which extensively shaped Estonia's attitudes. As a consequence, 2007 also served as a turning point for the EU in terms of shifting its approach to cyber policy from an economic to a national security issue. Furthermore, in 2008 Estonia was the first EU Member State to publish a broad national cyber security strategy. This had a cascade effect and it was followed by the publication of national cyber security strategies in 25 EU Member States:

- Estonia 2008 updated in 2014
- Finland 2008 updated in 2013
- Slovakia 2008 updated and valid for period 2015-2020
- Czech Republic 2011 (valid for the period 2011-2015)
- France 2011 updated in 2015
- Germany 2011
- Lithuania 2011 (valid for the period 2011-2019)
- Luxembourg 2011
- Netherlands 2011 updated in 2013

- UK 2011 accompanied by a Report on Progress in December 2014
- Romania 2011 updated in 2013
- Poland 2013
- Hungary 2013
- Austria 2013
- Spain 2013
- Italy 2013
- Cyprus 2013
- Latvia 2014
- Belgium 2014
- Estonia 2014
- Croatia 2015
- Luxembourg 2015
- Ireland 2015-2017
- Denmark 2015 accompanied by Digital Strategy 2016-2020
- Slovenia 2016-07

Adapted and updated to July 2016b from ENISA

The Estonian cyber attack of 2007 is among the most talked about and complicated cyber events of the last decade. It is a good illustration of how internet-based activities clash with governments and international governance in a way that promotes new organisational models across entire regions (Mueller, 2010: 18).

A number of cyber attacks, in the form of a wave of Distributed Denial of Service attacks (DDoS) were launched to overload various websites of the Estonian government, newspapers and banks over a period of three weeks (Cavelty, 2007). The attacks were carried out in protest against the removal of a Second World War monument (a bronze statue of a Soviet soldier) by the Estonian authorities at the end of April 2007 (Cavelty, 2007). In the midst of all the chaos, NATO and then the U.S.

National Security Agency (NSA) sent computer experts to Estonia to help them fight off the attacks and to find the source of the damage.

First, this failure demonstrates how both national police forces and legal systems struggle to deal with surges in online crime or attacks, since they only possess a limited amount of resource and expertise. Second, this case study reveals that the core overarching problem of developing effective cyber defence capabilities, in parallel with the issue of intelligence sharing, still lies in the prevalence of national interests among the Member States (Cross, 2011). Third, the EU reaction to the cyber attack on Estonia (or, to use Estonia's official term, 'cyber-riot') was relatively slow and the U.S. eventually turned out to be the driving force in the Western cyber-response. Furthermore, this case underlines not only the *lack of a clear division between the state and non-state actors* (for example, Microsoft-Europe, IBM-Europe) but also the lack of a coherent EU cyber security resilience plan that could be applied to any future cyber attack scenario.

There have, nevertheless, been some constructive developments during the eight years since the Estonian attacks in 2007, such as the EU Cyber security strategy, which was adopted in 2013, and the Network and Information Security (NIS) Directive, which required two years of negotiation and was finally agreed between the Council and the EU Parliament in December 2015. The NIS Directive is regarded as the first EU-wide legislation on cyber security with minimum obligations for all Member States and it will also oblige online firms, such as Amazon or Google, to notify of serious breaches or face sanctions (EurActiv, 2015c).

Germany:

The Federal Ministry of the Interior in Germany plays a central role in driving cyber policy in a similar manner to their approach to other fields of home affairs. In 2009, shortly after the events in Estonia, the Federal Office for Information Security (BSI) was redesigned. Currently, it focuses on providing ICT services and information security not only for the government but for the wider public as well (Nagyfejeo, 2012: 35). Germany is 'trying to follow a more civilian approach by placing greater emphasis on developing a cooperative connection between the private and public sector; therefore, the BSI cooperates closely with the private sector and the suppliers of information technology' (EU Parliament, 2011: 32, Nagyfejeo, 2012: 35). As a result, a better level of information sharing has been established in parallel with the expansion of the Critical Infrastructure Protection (CIP) implementation plan. In 2011 the German government proposed the creation of a National Cyber Response Centre (NCRC) and National Cybersecurity Council 'with the aim of optimising operational assistance between state authorities, and improving the awareness of cyber threats', and these proposals were outlined in the *Cybersecurity Strategy for Germany* (Federal Ministry of the Interior, 2015). The NCRC – operational since April 2011 – sends 'reports to the BSI while also collaborating with the Federal Office of Civil Protection and Disaster Assistance (BBK)' (Federal Ministry of the Interior, 2015). All of these factors show that Germany is in the process of setting up cyber forces, although the level of cyber security preparedness is still lagging behind that of the UK (Nagyfejeo, 2012: 35).

In addition, in August 2014 the Interior Ministry disclosed tough new cyber security measures with the introduction of a 'draft cyber security law' to protect the critical

infrastructure in Germany. In the report called *Die Lage der IT-Sicherheit in Deutschland 2014* the BSI acknowledged that an iron plant was physically damaged by a cyber attack, which caused a security breach in the plant's control system, and this incident provided more justification for these actions (King, 2014). Some consider this to be the first successful cyber attack on critical infrastructures (Beshar, 2015). Other goals include ensuring the protection of IT systems and citizens generally, with the aspiration that the German digital infrastructure will become the 'safest in the world' (German Federal Ministry of the Interior). Furthermore, because cybercrime poses an increasing threat, according to the Interior Ministry 'IT security is a top priority, because an IT failure could compromise Germany's internal security' (German Federal Ministry of the Interior, 2015).

From the point of view of strategic culture, the federal government is still the most vital player in all German foreign and security policy, including cyber policy. According to Junk & Daase, transatlantic and European trends, such as the European Cybersecurity Strategy introduced in February 2013 and the Commission's Network and Information Security (NIS) Directive, have a great influence on German security policy. However due to the fragmentation within the German government over general foreign policy style, Berlin's reaction to European and transatlantic policies remains unpredictable (Junk & Daase, 2013: 149).

***France*:**

In France, the focus is to prioritise the French language, and therefore 'the security concerns of the country are separate from those of many other countries as more of the web systems and websites are national' (Nagyfejeo, 2012: 34). France exemplifies

one of the key difficulties faced by European countries, namely that the needs of local bodies must be taken into account, which can result in incapacity to collaborate at EU level. The role of local bodies is, however, of particular importance as local bodies allow 'the Member States to monitor and control the different levels of cybercrime in their countries' (Bertsch 2001: 246-249; Raitman 2005: 702-706; Nagyfejeo, 2012: 34). The *French White Paper on Defence and National Security* presented by the President in 2008 was the first important document that highlighted the importance of information system security (ENISA, 2014). As a consequence, in 2009, the French Network and Information Security Agency (ANSSI) was created with the 'aim of coordinating the information security of governmental networks, institutions, companies and individuals' (Nagyfejeo, 2012: 34). Furthermore, since 2011 this agency has identified four more goals:

- to increase cooperation with the private sector
- to connect local cyber defence with global cyber power
- to expand cryptographic measures within the French CIP and NATO
- to prevent theft of identity (ANSSI 2012; Nagyfejeo, 2012: 34).

The combination of these steps has resulted in one of the most developed cybersecurity plans in Europe, particularly as France intends to incorporate both its cyber defence and offence capabilities seamlessly with its traditional forces (ANSSI 2012).

United Kingdom:

By contrast, the UK takes a rather business driven approach to the way it deals with the private sector, giving priority to voluntary reporting mechanisms, and it can be regarded as the Member State with the most similar cyber approach to the U.S. One of

the drivers of the UK voluntary approach is the Department for Business, Innovation and Skills (BIS) '(…) With regard to the legislative approach being taken in the EU, our approach will inform the voluntary and collaborative UK position' (BIS, November 2013). In the USA there is also a very close exchange with industry but ultimately this is driven by different types of government agencies like the Department of Homeland Security (DHS), the Department of Defence (DoD), Department of Justice (DoJ) and the Federal Bureau of Investigation (FBI).

The similarity between the UK–U.S. approaches to tackling cyber threats is not particularly surprising. Cornish argues that from a strategic culture perspective, the UK–U.S. alliance has been strong at both the national policy level and in terms of operational activity, as both countries have a long history of converging intelligence and security activity, beginning with the BRUSA treaty governing exchange of military signals concluded in 1943 and further elaborated over the next ten years (Cornish, 2013: 377). The twin pillars of the U.S.–UK special relationship are intelligence and nuclear cooperation, and the UK has managed to develop a robust submarine-based nuclear deterrent force as a result of its long-term cooperation with the U.S. (Cornish, 2013: 377).

The U.S. has pursued a new stream of cyber security cooperation with the U.K. that further supports the argument for the existence of a U.S.–UK special relationship. In January 2015, both President Obama and Prime Minister Cameron clarified their commitment to enhancing the cyber security of their critical infrastructure, to improving the sharing of threat information and to bilateral intelligence collaboration on cyber issues (White House, 2015a). Cameron also highlighted his intention to take

specific action in creating links with industry and therefore mobilising industry to fight cybercrime. Although both countries are part of the "Five Eyes", the existence of a more exclusive U.S.–UK special relationship is further exemplified by the latest developments; the creation of a joint cyber cell that is operating in both countries.

[Table 3.2.]: *U.S. vs. UK*

UNITED STATES	UNITED KINGDOM
Computer network defence - information sharing – cyber incident management	
U.S. Computer Emergency Readiness Team (US-CERT)	CERT-UK
National Security Agency (NSA) Federal Bureau of Investigation (FBI)	United Kingdom's Government Communications Headquarters (GCHQ) Security Service (MI5)
Joint cyber cell – stimulated attacks for testing	

Source: BBC, The Guardian, White House, 2015a

Compared to France and Germany, 'the UK has already dealt with a wide range of cyber defence issues and since 2010 it has aimed to expand what are clearly the most extensive cyber defence capabilities in Europe', focused mostly on the Cabinet Office and Government Communications Headquarters (GCHQ) (EU Parliament, 2011: 33, Nagyfejeo, 2012: 35). This has mainly occurred because the UK recognised early that a resilient internet is of importance to the financial services industry. The decline in the manufacturing industry has made the UK very dependent on the financial sector, so the security and reliability of systems used by the banks, government institutions and other bodies needs to be protected (Nagyfejeo, 2012: 36).

The rapid growth of cybercrime is a significant barrier to many of the businesses that are working to improve their productivity. Accordingly, the overarching aim of the UK government has been to ensure that, at a local level, 'security procedures are followed and that companies can access security advice at all times' (Cabinet Office 2011; Nagyfejeo, 2012: 36).

The UK cyber security strategy is also based on a number of key propositions (Nagyfejeo, 2012: 36). The UK approach recognises the need to engage with other countries in order to combat cyber attacks. This has required the UK's main government centre for electronic security to reorient itself, moving from an inward facing department that protected the communications of government departments and diplomats to an outward facing organisation that commands the confidence of business and industry. To achieve this, the country's strategy has been to develop infrastructure and other facilities, which provide assistance, and also to ensure that the long term needs of the civilians can be fulfilled. A core issue from this perspective is the manner in which cyber security issues have been dealt with at the national level (Nagyfejeo, 2012: 36). One of the most important issues that has been addressed within the UK is to ensure that there is a reduction in the level of risk of disruption to local systems through cybercrime (Cabinet Office 2011, http://www.cabinetoffice.gov.uk). Therefore, while the UK government, in partnership with industry, has managed to 'integrate different departments to work together on a number of initiatives', there is a clear lead department upon which technical competence is focused (Cabinet Office, 2011).

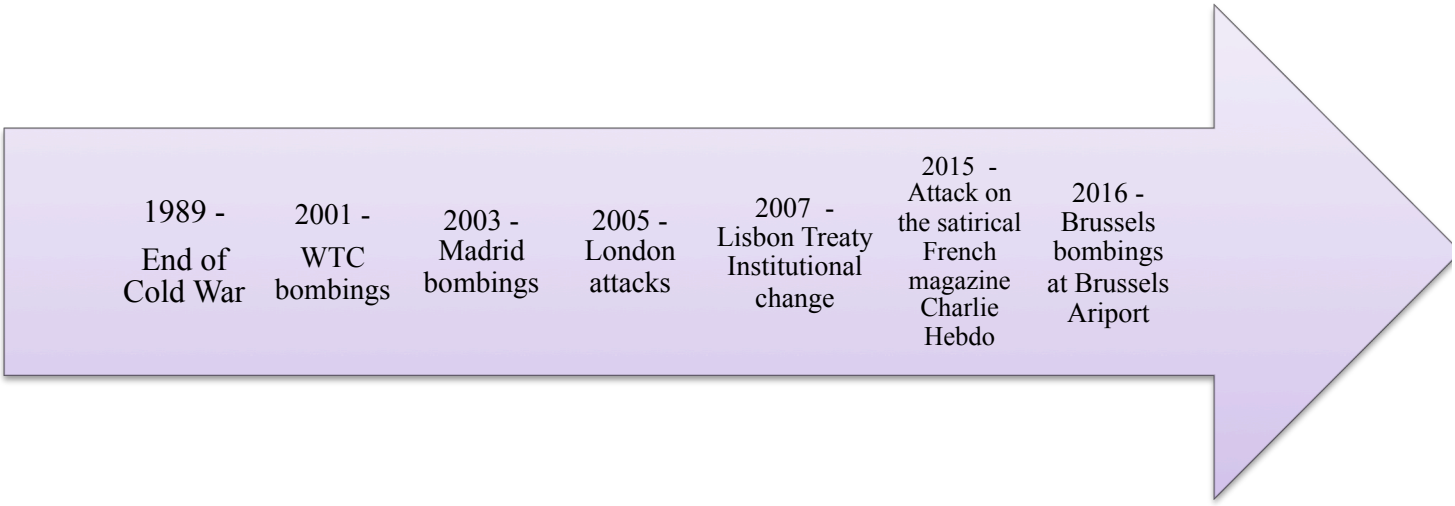
The first UK National Cyber security Strategy was published in 2011 and three years later London issued a progress report tracking its work towards four strategic objectives including:

> (1) the enhancement of resilience against cyber attacks;
> (2) making sure that the UK is one of the most cyber-safe countries in the world for both businesses and citizens;
> (3) raising cyber security awareness through education and the promotion of capabilities and training;
> (4) the support of open societies (Cabinet Office, 2014, www.gov.uk).

Cabinet Office Minister, Francis Maude, who presides over cyber security, stated that 'as part of this Government's long-term economic plan we want to ensure that Britain is one of the safest places to do business online… with Alan Turing and Bletchley Park, the UK has a proud heritage in cryptography and computer science' (Cabinet Office, 2014, www.gov.uk).

There is a widely held assumption that the diverse national strategic cultures across the EU are the cause for the lack of consensus among Member States. This challenge presents obstacles when it comes to cyber security collaboration, not just within the EU but also with international partners such as the U.S. It has been suggested that the organisation of defence has been hampered by the absence of a strong European strategic culture, and this absence, can be attributed to the lack of a core set of European values, which could foster convergence (Bailes, 1999; Biavi et al., 2011: 1230). Certainly divergent military doctrines and traditions serve as a further explanation as to why there is still no White Paper on the EU's security and defence.

Additionally, it could be argued that convergence is possible because the EU's strategic culture is not static, and as Meyer, Lantis and Pirani argue, it is exposed to constant challenges and 'shocks'. Meyer has outlined some shocks and pivotal events in strategic culture that triggered changes in EU security policy (Meyer 2001, 2003 (Madrid) 2005 (London) and 2007 (Lisbon Treaty)). Despite the fragmented nature of EU strategic culture, the NIS Directive (discussed later), the revised General Data Protection Regulation (GDPR), and the new 2013 Directive on attacks against information systems have all been developed. These demonstrate that there have been significant developments in EU cyber security, even though progress is tentative.



[Figure 3.3.]: *Shocks and pivotal events that triggered changes in EU security policy*

In essence, the CSDP *is considered to be the backbone of European strategic culture*. However, it is important to note that the CSDP was created as a self-consciously 'sovereignty-sensitive' intergovernmental structure by Member States, and it provides Member States with the flexibility to decide upon the extent to which they are willing to participate in and implement certain elements (Biava et al, 2011: 1230). Therefore, CSDP is not under the direct control of supranational bodies like the Commission, the Parliament or the Court thus cannot facilitate the promotion of a strong EU strategic

culture. Biava formulates this neatly as an EU paradox: 'centralized authority would have the capacity with no legitimacy whereas national institutions have the legitimacy but without adequate capacity' (Biava et al., 2011: 1230).

Differences in strategic cultures across EU Member States present not just an abstract problem, but also serious moral and ethical dilemmas in terms of practical international collaboration. For instance, from the German government's point of view, any restriction would *harm freedom* of speech and would be regarded as the first step towards internet censorship. This is closely aligned to the U.S. approach, as they also wish to maintain an open and free internet, championing freedom of speech as set out in the First Amendment. The German internet policy experts' solution is therefore to use legal measures for deletion, not blocking (Bölinger, 2014). In contrast, the UK is in favour of blocking illegal content from the internet and this divergence could be explained by the different historical path both British and German citizens followed during the twentieth century. This also explains why the UK has zero tolerance towards the issue of child sexual exploitation online. Any image of child abuse is treated as unlawful and therefore ISPs and search engines immediately remove such images as soon as they become aware of them. To illustrate, according to the 2013 Internet Watch Foundation (IWF) Report '47% of UK hosted child sexual abuse content were removed within less than 60 minutes from when a takedown notice was issued in 2013. The quickest was 2 min and 39 seconds.' (IWF, 2013: 7). A better solution would be to carry out these actions at a European level so that the victim is not re-abused in a different jurisdiction (Interview, 2014b).

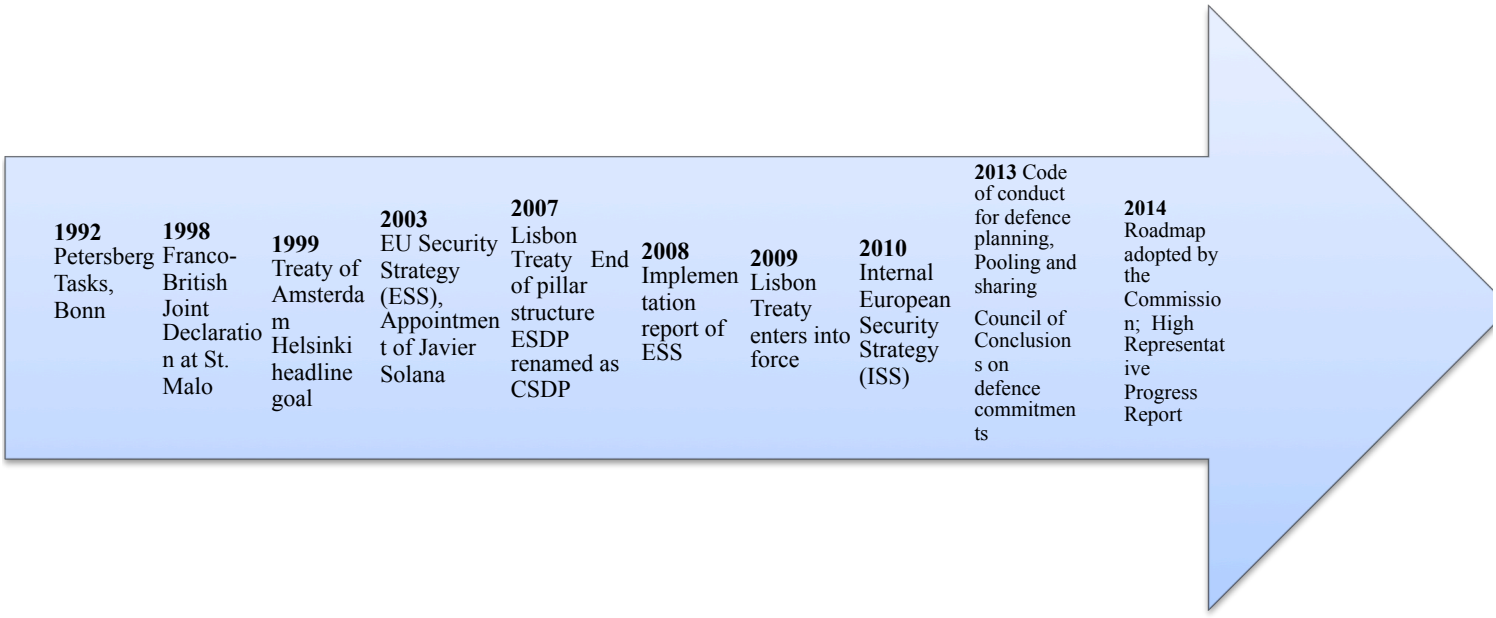
1.5. Historical formation of CSDP – EU perception of threats

Before analysing cybercrime and its position within various institutions of the EU, its context must be considered by examining the progression of EU strategic culture. This will be addressed by considering the evolution of the CSDP, formerly known as the European Security and Defence Policy (ESDP). Current literature on EU strategic culture has focused on the CSDP and accordingly this chapter will move on to link CSDP with cyber defence as this is an increasingly urgent issue in EU cyber diplomacy. While cybercrime is not the same as cyber defence, nonetheless, a short overview of cyber defence will assist with benchmarking the mechanisms of EU cyber security policy from a strategic culture perspective.

The development of the EU Common Foreign and Security Policy (CFSP) clearly indicates that the norms and progress of CSDP helped to stimulate the formation of EU strategic culture by connecting the use of force with wide-ranging civilian-military policy instruments (Biava *et al*., 2011: 1237). Because the dominant literature reveals a strong consensus linking the development of EU strategic culture with the CSDP, this will be the starting point. A levels of analysis approach will be used, and cyber defence as a strategic issue will be linked to the policies of Brussels in areas where cyber security operates, before this is associated with the more operational realm of cybercrime. It will be argued that the development of *EU strategic cyber culture* has been shaped not only by defence, but also by the institutional and legal policies, the changes in strategic culture and the 'division of labour' with NATO, a vital pillar of Europe's security architecture.

The first important step in the creation of the ESDP was the *Petersberg Tasks* agreed in 1992 near Bonn, Germany. These defined situations in which EU troops are deployable which include humanitarian and rescue tasks, peacekeeping operations (PKO) and crisis management. This clearly shows that, with the exception of humanitarian type missions, the EU military remains inadequate.

Nevertheless, aspirations in this realm are long-standing. The 1998 *Franco-British Joint Declaration on European Defence* at Saint-Malo acknowledged the need for an autonomous EU defence capacity, whilst making sure that NATO obligations and commitments are not violated (Cornish & Edwards, 2011: 807). The Treaty of Amsterdam (which came into force in 1999) increased EU responsibilities concerning humanitarian work and peacekeeping, however it did not create a common defence policy (Biave et al., 2011: 1241). Developing a deeper understanding of the *EU institutional culture* by reviewing the major decisions taken under the CFSP umbrella might serve as a better indicator when analysing the decisions taken to develop a common EU response to external threats.



[Figure 3.4.]: *Evolution of strategic guidelines of the European Common Foreign and Security Policy (CFSP)*

Adapted and updated to December 2014 from Biava et al. (2011, Table 3. pp. 1241-1243)

The EU's approach to security and threats was formulated under CFSP, materialised within ESDP and has been referred to as the CSDP since the Treaty of Lisbon 2007. What do these agreements tell us about an emerging European strategic culture? Importantly, the European commitment to using military deployment only for humanitarian missions, reconciliations and to protect assets/systems used in operations, can be linked to the *EU's identification with the Kantian idea* of pursuing national security and economic interests through diminished fighting of wars.

Most scholars of strategic culture agree that the most significant EU strategic document to date is the European Security Strategy (ESS), adopted in 2003. This is also regarded as the point at which a specific type of EU strategic culture, with a meaningful and detailed texture, was created (Toje, 2009). It has been widely regarded as a breakthrough in the evolution of EU's security and foreign policy, since Member States displayed a wide consensus on how to identify common threats and how these should be tackled (European Council, 2003). In some ways ESS can be considered as an embryonic equivalent to the 2002 National Security Strategy implemented in the U.S. insofar as it was created from consolidation of existing views and practices (Norheim-Martinsen, 2011: 518).

Strategic documents like the European Union's Security Strategy (ESS) have been vital in terms of disseminating, regulating and systematising key shared norms of EU strategic culture, although many criticised it for not, in fact, being very strategic.

Javier Solana, the former EU High Representative for the CFSP, argued that the clear objectives and core values set out in ESS represent a 'strategic culture that fosters early, rapid, and when necessary, robust intervention' (Toje, 2009: 9; Cornish & Edwards, 2011: 801; European Council, 2003). Not everybody found this convincing, nevertheless, some argue that the EU strategy outlined in both 2003 and 2008 failed to tackle the core questions of defence (Haine, 2011: 584).

Under the French Presidency, in 2008, the ESS implementation report, entitled *Providing Security in a Changing World*, was presented, and it paved the way for discussion about methods for implementation and the further tasks still required. It was also fundamental in that it led to the creation of a 'new civilian-military planning structure for CSDP operations' that was agreed by the Member States (Biava, 2009). Again, these steps also helped to promote the civilian-military nature of EU strategic culture, which was underlined by the subsequent creation of the Crisis Management and Planning Directorate (Biava *et al*., 2011: 1237).

Lagadec reflected that 'the EU does not draft a European Security Strategy in order to determine how it will act, but *who it is*' (Lagadec, 2012: 32). This further implies a certain vagueness of strategic vision and the amorphousness of methods used when confronting crisis. According to Heisbourg, the composition of an EU white paper on defence is fundamental for the presentation of EU military doctrine and for crystalizing the military aspects of EU internal security (Heisbourg, 2004: 36). Therefore, some claim that as the ESS strategic documents have failed to define the exact role of the EU as a global security actor, the real criterion for a credible culture

would be the development of a *defence white book for the CSDP* (Biscop and Norheim-Martinsen, 2011: 74). Meanwhile, Larivé notes that due to the ongoing debate about what amounts to a present threat, nothing was in place to push against, so the CSDP was left without a coherent strategy (Larivé, 2014: 133; Merlingen, 2012: 89). In other words, if the EU is not going to come up with a defence strategy beyond guidelines for intervention and crisis management it will be difficult to implement this operationally, still less formulate force structures.

The requirement for a further development in EU foreign policy is demonstrated in the new EU Global Strategy on Foreign and Security Policy (EUGS) that has an ambitious goal: to embody and recognize the shared interests of all the 28 Member States in terms of foreign policy with all other regions and in all significant policy fields (Techau, 2016). However, the main difficulty in achieving this relates to determining the common interests of the actors that Techau argues is 'part of the internal power game' (Techau, 2016). Therefore, the critical question of whether the EUGS will be nothing more than a paper tiger, which is how Bures referred to the EU counterterrorism policy, is still debatable (Bures, 2006). Others suggest that the document will serve more as a guideline rather than a concrete or prescriptive order.

These wider questions of EU security culture beg the question as to whether a similar path can be traced in the development of EU cyber defence policy. It is difficult to examine the issue of cyber defence policy without talking about regulatory frameworks, since a nation's culture and heritage can often be traced through the formation of laws. However, EU cyber defence issues are still in development and national legislatures exhibit a lack of experience relevant to the delimitation of

today's technological advances surrounding privacy and the approach to legislation for a resilient communications infrastructure. Therefore, there are multiple problems, not only do Member States have different cultural backgrounds, but there is also a lack of stability within the various national services, making it even harder to create a unifying doctrine. Consequently, the EU cyber defence policy issue is further complicated as most EU countries lack coherent national doctrines relevant to fighting wars in cyberspace and have little understanding of how this new realm relates to their traditional "ways in warfare" (Andress, 2011: 242).

1.6. Evolution of EU strategic cyber culture

The following sections will discuss the non-static nature of the way in which strategic cyber culture can evolve (and potentially converge) at the EU collaborative level – even when intergovernmental institutional modes of governance are dominant. This thesis suggests that the linkage between CSDP and cyber defence could be regarded as a starting point in the development of EU strategic cyber culture. The reasoning for this linkage with defence is based on current literature that connects CSDP with EU strategic culture. Yet, this research will not ignore the fact that EU level cyber defence is still a "greenfield" area and the least mature pillar of EU strategic cyber culture. It is argued here that the CSDP can offer both a starting point and a means for transition from the traditional into the cyber aspects of strategic cultures. This will also help us to understand the fragmented nature of EU cyber cultures that have been developed on the policy, legal and operational levels. For instance, policy initiatives on information security, infrastructure protection and the different aspects of cybercrime were coordinated under the comprehensive EU Cybersecurity Strategy (2013) while cyber defence is organised under EEAS and EDA (Robinson, 2014). In

essence, cyber defence was a priority area outlined in the EU Cybersecurity Strategy so they are not separated strategically, but are in terms of governance and institutions. While not all the Member States participated in these cyber defence developments, some, including the UK, who previously refused to participate, have gradually come to see the importance of these developments.

Therefore, in order to understand the development of EU strategic cyber culture, the following section is going to explore the linkage of CSDP to cyber defence.

Stage One: CSDP linked to cyber defence

Having reviewed the way in which the CSDP has been developed so far, it is obvious that it is not yet the 'cornerstone' on which a strong and shared EU strategic culture could be built upon. Therefore, at present, EU strategic culture serves only as a supplement to national strategic cultures (Schmidt & Zyla, 2013: 41). According to Hyde-Price and Peter van Ham, wars have always had a disproportionate effect on shaping national strategic cultures. Paradoxically, because the existence of the EU has contributed to an absence of war in Europe, it is unlikely that a strong EU strategic culture will develop (Hyde-Price, 2004; Peter van Ham, 2005). It may be that EU expansion, combined with the controversies over the Ukraine in 2015 and 2016, may accelerate its emergence. However, it could be argued that the presence of war and robust EU military operations should not be regarded as the only factors that can determine EU strategic culture. Precisely because of the nature and complexity of the EU, its strategic culture is not necessarily limited to the use of force, but may extend to the security aspects of trade, diplomacy, foreign policy, culture, law and technology. Indeed, many scholars working on EU foreign policy acknowledge the

EU's international actorness and recognise that its strength also comes through trade and economic diplomacy (Smith, 2004; Manners, 2006). The effectiveness of the EU's foreign economic policy also raises serious questions relating to the civilian and normative power of the EU (Duchêne, 1973; Manners, 2002; Diez & Manners, 2007).

Stage Two: CSDP – a cyber defence paradox

In the realm of cyber security something of a paradox has emerged.

According to one senior NATO official, with the possible exception of Britain, the U.S. never intended to export cyber technologies widely to its European allies (Interview, 2014c), yet, the presence of an American lead has still deterred the emergence of a distinct European approach. The paradox is, however, that the U.S. have made their European allies comfortable by keeping them in a position of a degree of dependence (this resulted in the creation of the ESDP, later named CSDP), whilst simultaneously maintaining a constant pressure on their allies, in order for the U.S. to increase their budgets for defence. According to Rees, another reason for this U.S. behaviour was, at least in part, because Washington misjudged the EU efforts to improve defence capacity and regarded ESDP as a threat to NATO and a possible road to European autonomy which the U.S. wanted to avoid (Rees, 2011: 64).

In other words, the story of *EU cyber defence is not all that different* from CSDP. Whilst the issue of cyber security plays an important role in the EU's Internal Security Strategy (ISS) – a strategy that is currently undergoing a process of renewal for 2015–2019 – there has been limited EU action within the scope of the CFSP, partially due to the reluctance of Member States to collaborate on this matter. The reasons for this reluctance can again (similar to the CSDP problem) be explained

fairly easily. Due to the limits of the authority of CFSP and also because of the traditional great degree of reliance on the U.S. for military and defence, Member States tend to choose cooperation with NATO instead. There is also a reluctance to duplicate effort during a period of budget shortages. Some even argue that this type of 'division of labour' between the EU working on the civilian aspects of cyber security and NATO on the military aspects is the most sustainable approach in the long-term (Interview, 2014d).

The EU has so far failed to carry out what might be termed as a fully incorporated civil-military operation, and EU strategic culture does not currently appear sufficiently robust to tackle these problems. This might change once all European troops are withdrawn from Afghanistan, which will liberate greater resources (Schmidt & Zyla, 2013: 46). Nevertheless, EU cyber defence is unlikely to become the 'lifeblood' of EU strategic cyber culture mainly because it is not about developing cyber offence – or cyber offensive weapons whereas CSDP has been about to develop a military presence (especially since St Malo) as well as civilian. EU cyber defence is still in its infancy, however this does not mean that an existential shock - such as a massive cyber attack on European critical infrastructures[6] (for example, the energy and transport sector) - might not trigger a significant boost in EU cyber defence expenditure. Despite these strategic observations, the progress that has been made on EU cyber defence during the last five years on a day-to-day basis should not be overlooked.

[6] "European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States", in Council *Directive on European critical infrastructures*, 2008/114/EC.

Stage Three: EU cyber defence policy framework: deterrence by resilience

The genesis of the current EU cyber defence policy framework can be regarded as a further development or elaboration of the EU cyber security strategy published in February 2013. In much the same way as Bures criticised the EU counterterrorism policy as nothing more than a "paper tiger", during interviews, some EU officials indicated that, while the EU cyber security strategy is an impressive document, it is, to begin with, only a paper, or perhaps an aspiration (Bures, 2006: 73). However, as if to confound critics like Bures, the EU counterterrorism policy continues to grow incrementally and to command growing engagement from both national agencies and the Counter-Terrorism Group, a body of all European security services (Aldrich, 2012). Using this analogy, one might observe that a strategy 'survives' and grows depending on the way it is implemented. According to an EDA official, the EU cyber security strategy has been accomplished in a very transparent way and published worldwide, which indicates one way of building confidence for external partners. Accordingly, it is likely to build slowly but progressively over time as partners gain confidence and establish joint working habits (Interview, 2015a). Some might argue that this is a classic liberal institutional pathway, gathering momentum over time.

A close review of the EU cyber security strategy reveals several strategic priorities, moreover, different levels of generality can be identified throughout: while the civilian aspects include very detailed actions, the cyber defence side (that is the part over-lapping with the CSDP), by contrast, is relatively generic. This can be explained by the fact that EU-led military operations currently rely fully on Member State capabilities, and this extends to both cyber defence and conventional CSDP operations.

Cyber defence activities are located within the EDA that was created in July 2004 in order to foster cooperation and remedy some of the shortages in European defence capabilities (Cornish & Edwards, 2005: 805; Rees, 2011: 76). Essentially, the EDA is in charge of EU cyber defence policy matters and it is therefore the task of the EDA to consult with the Member States to identify their intentions and capacities beyond the outline strategies. One of the challenges that the policymakers had to face concerning the EU cyber security strategy was how to move from the high level of generality present in the strategy to a very detailed level of concrete actions regarding cyber defence. This difficult task was addressed by the EU Cyber Defence Policy Framework, which was mandated by the European Council Conclusions on CSDP in December 2013 and agreed by the Foreign Affairs Council in November 2014.

The objectives of the EU Cyber Defence Policy Framework (See figure 3.5, below), based on the EU cyber security strategy and the Council conclusions, might be visualized as follows:

[Figure 3.5.]: *EU Cyber Defence Policy Framework*
Source from EDA, www.eda.europa.eu

- to identify the priority areas of focus for CSDP cyber defence from personnel, technical and procedural perspectives
- to clarify the roles and responsibilities of different institutional players and Member States within cyber defence in CSDP operations
- to integrate cyber defence in the management of external crisis - the approach was thus not to establish a new cyber crisis management system but to find a way to integrate it into the existing crisis management mechanisms
- to outline the principles for cooperation with the private sector, in other words, acknowledging the role the private sector plays (they are the largest stakeholders in cyberspace and they are also the major operators) since there is an enormous potential for civil-military cooperation ("dual-use") and civil-military synergies in the area
- to ensure consistency between NATO and EU cyber defence efforts

(EDA, 2014)

Some of these strategies may seem to have little operational substance, however, they are nevertheless indicative of extensive discussion and serious reflection. With regard to cyber defence, Zyla argues that elites tend to 'homogenise norms' that are then communicated to the other members of society (Zyla, 2011: 672). It could therefore be argued that strategic documents, such as the EU Cyber Defence Policy Framework (2014) and NATO's enhanced Cyber Defence Policy (2014), contain a distillation of the normative viewpoints of the industry leaders about negotiation outcomes and the bargaining process, and their values, norms and strategic beliefs about cyber defence including a rationalisation of government actions (Zyla, 2011). Neumann and Heikka also remind us that such elite political documents embody information about the 'processes that social actors learn from their peers' and are therefore worthy of sustained analysis (Neumann & Heikka, 2005: 6; Zyla 2011). The Technical Arrangement on Cyber Defence was established between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU) in February 2016, and it demonstrates that both the EU and NATO can collaborate effectively on matters of mutual interest, such as protecting their networks and sharing best practices and information between the emergency response teams (NATO, 2016).

Stage Four: EU Cyber Defence and CSDP – same destiny?

When the historical evolution of the cyber defence activities by the EU and NATO are compared and contrasted, it is clear that NATO 'enjoys' pre-eminence. In 1999, NATO put cyber defence on its agenda for the first time following the cyberattacks against NATO during the Kosovo war. In contrast, it was not until November 2014

that the Foreign Affairs Council adopted the first EU Cyber Defence Policy Framework (Terlikowski & Vyskoc, 2013). After 1999 the following key developments occurred in NATO relating to cyber defence:

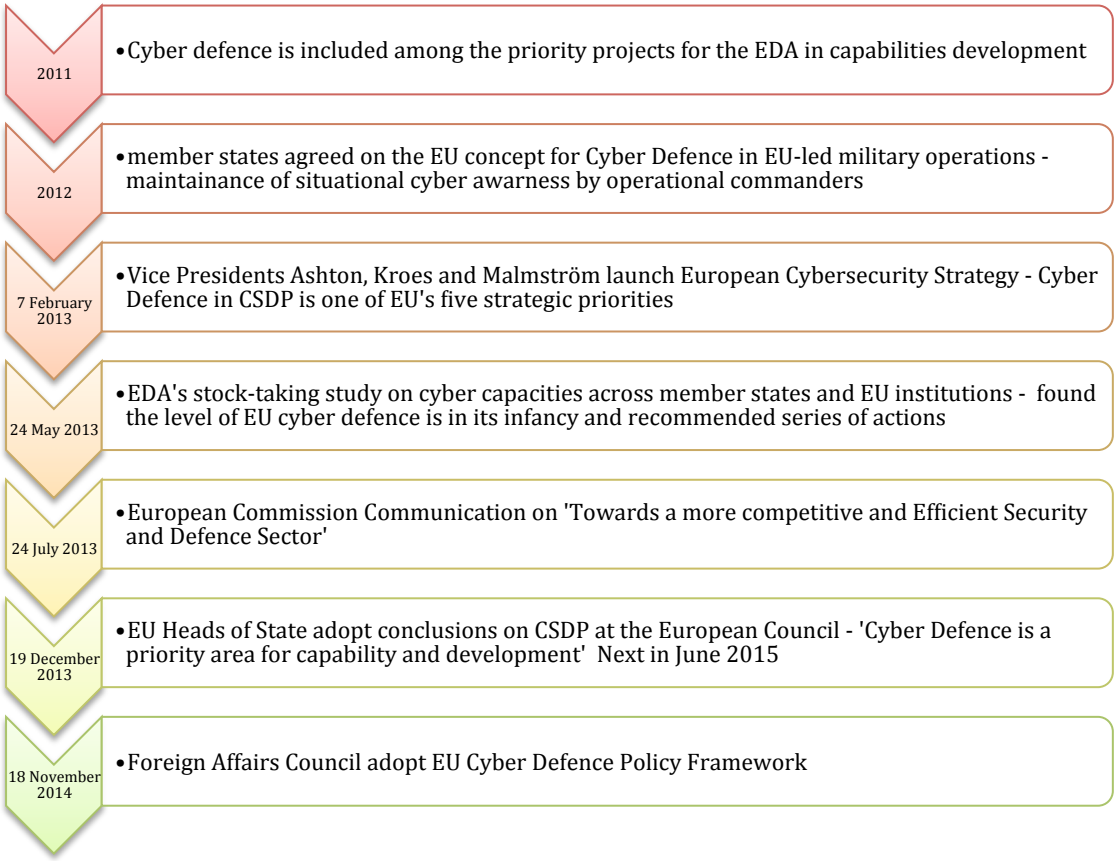
- 2002: NATO adopted a cyber defence programme and created the NATO Computer Incident Response Capability (NCIRC)
- 2008: NATO Cyber Defence Policy was approved by the NATO leaders
- 2010 (Lisbon Summit): cyber defence was integrated into NATO's defence planning process
- 2011: NATO approved its revised Cyber Defence Policy and Action Plan

Ambassador Iklódy, NATO's former Assistant Secretary General for Emerging Security Challenges, clearly emphasized NATO's two-fold role at a cyber meeting hosted by the Royal Military Academy in Brussels in June 2013: 1.) Defending networks it owns and operates (centralizes) 2.) Collective defence organisation (Art. IV.) by making no distinction between traditional and cyber attacks (Iklódy, June 2013). In other words, protection is primarily a national responsibility, with investment seen as a duty of the Member States, with NATO providing support and assistance. Although NATO only focuses on defending its own networks in cyberspace in September 2014, during the NATO Summit in Wales, the Allies nevertheless approved an initiative to 'enhance cyber defence policy' well beyond this narrow remit. This was done by the rather radical step of endorsing the possibility of invoking Article V of the Washington Treaty, which relates to collective defence, in case of a cyber attack, thus associating it with an 'armed attack' in certain circumstances (Healey & Jordan, 2014: 6). There is, nonetheless, no clear indication of the type of conditions in which an Article V response would be activated or whether the response would be a traditional military intervention or virtual.

Specifically, the North Atlantic Council would be responsible for deciding, on a case-by-case basis, the form of response NATO should take against a cyberattack (Interview, 2014e). According to a NATO official, although operational coordination would remain within NATO, the response method would still depend on how much sensitive knowledge about offensive capability various Allies would be willing to reveal to each other (Interview, 2014e).

The characteristics of the discussions in autumn 2014 raise several questions. It is clear that NATO (having the U.S. on board) has already been the frontrunner in terms of developing cyber defence capabilities. Therefore, it might be assumed that the EU's own cyber defence capacities, led by the EDA, might always be over-shadowed by NATO and as such may perhaps represent a diversion of resource. It is important to note though that NATO and EDA do not regard themselves as competitors and engage in a non-zero-sum game. Indeed, there has been some positive informal coordination between EU and NATO officials on cyber security. Having the EU accessing NATO cyber defence capabilities for operational purposes could be an opportunity for a fruitful practical collaboration (Robinson, 2014). However, the possibility that this attitude might change cannot be excluded, since there is still no agreement between the Member States regarding the creation of a sustainable cyber defence capacity for NATO that could help an ally (Círlig, 2014: 9). Furthermore, NATO currently focuses on the defence of its own networks and as a result encourages the allies to develop their own cyber defence networks and manage their related national activities. This is undoubtedly due to the reluctance of countries to discuss their cyber offensive capabilities even with their closest European allies, not least because they raise issues of legality.

In addition, NATO focuses predominantly on its military networks, which are also dependent on civilian infrastructures. The consequences of a cyber attack scenario are blurred and therefore cyber interoperability and security standards are needed. Consequently, maintaining the separation lines between the public-private, civilian-military networks might not be effective.



[Figure 3.6.]: *Timeline of political-strategic framework for EU cyber defence in CSDP*

Adapted and updated to March 2015 from EDA

2. Strategy/policy dimension of EU strategic cyber culture

2.1. EU approach to cyber security

The EU has already indicated its preference for a *regulated* approach to cyber security by advocating the development of an internal "digital" market. In 1993, the EU White

Paper on “Growth, Competitiveness, Employment” and the Bangemann Report both referred to the creation of a common e-market (Commission of the European Communities 1993). The main goal of these documents was to eliminate obstacles that might hinder this development, while also taking into account issues such as privacy, computer security and intellectual property (Europe and the Global Information Society 1994). Remarkably, it was not until 2005 that the first law was adopted by the Council “on attacks against information systems” (Council Framework Decision 2005; Porcedda 2011). The U.S. approach thus benefited from “first mover advantage” by more than a decade, while it also promoted a *laissez faire* approach. Internationally, the U.S. has been an advocate for the economic benefits of a loosely controlled but robust network infrastructure which favours innovation and access for all to internet provided services (Arnas, 2009: 127).

The EU’s regulatory path toward the legislation of information security has been present in various forms across their mandates. For instance, the protection of information infrastructure was already emphasised in the *eEurope* Initiative in 1999 and the EU’s *Communication on Network and Information Security* in 2001 (Christou, 2015: 121).

According to Houdart, the EU has focused on the following three main pillars in order to enhance cyber security:

In 2004 the first pillar was initiated when ENISA was established with the aim of identifying cyber threats and protecting the Critical Infrastructures (CIs) of Europe. Progress had already been made with the organisation of the first pan-European cyber security exercise in 2012 (to test the preparedness of financial and government

institutions) and the publication of annual cyber incidents in 2011 (Nagyfejeo, 2015: 159).

In 2010 the second pillar, the Digital Agenda for Europe (initiated by the EU Commissioner for Information Society and Media, Neelie Kroes), placed a new emphasis on a number of legal procedures that would help to advance the socio-economic opportunities offered by the digital world (for example: e-commerce, e-signature and the protection of intellectual property (IP)) (European Commission 2010b; Nagyfejeo, 2015: 159).

In 2013 the third pillar – manifested in the establishment of the Cybercrime Centre as part of Europol – was directed by the EU Commissioner for Justice and Home Affairs, Cecilia Malström. This centre focuses on the active prevention of threats emanating from cyberspace, the investigation of crimes committed online, and the sharing of information among the European law enforcement and intelligence agencies (Houdart 2013; Nagyfejeo, 2015: 159).

Since 2004, ENISA has been attempting to assist and coordinate with Member States in the development of their own cyber security strategies, although a major hurdle remains the differing strategic cultures and views on cyber threats. The decision in 2013 to prolong ENISA's mandate for a further seven years can, according to its executive director Udo Helmbrecht, be considered a vital step "in the political process that enables ENISA to work more intensively on prevention and preparedness in the field of cyber security" (Business Insurance, 2013). A high-ranking official at ENISA confirmed that the major decision-makers over the extent to which power should be granted to ENISA are Germany and France, and they avoid granting more authority on cyber security to ENISA than national authorities have. In other words, Member

States fear encroachment into what they see as their national sovereign domain (Interview, 2015b). Even ENISA's second mandate only granted minor operational responsibilities despite many calling for it to be given the resources to become operational (Christou, 2015).

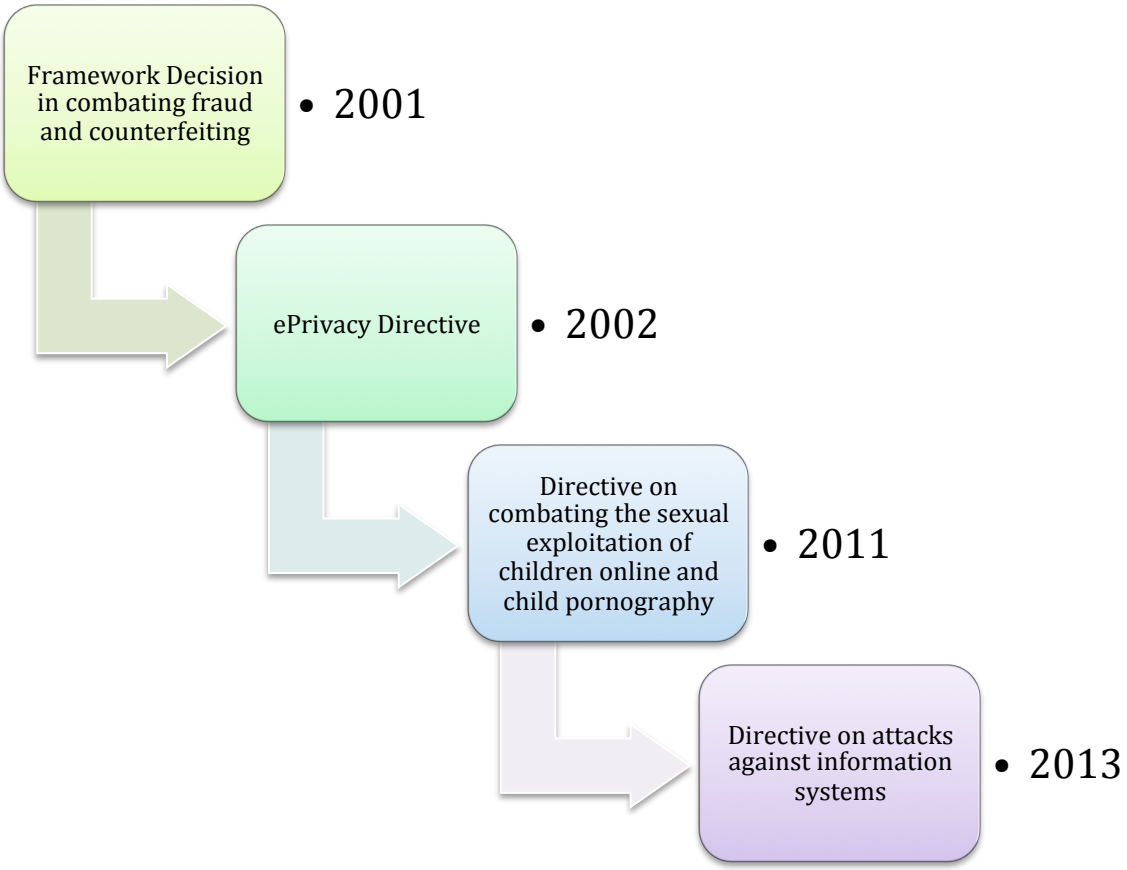
[Figure 3.7.]: *EU approach to cyber security*

Source: Borrowed from Paul Timmers, DG Connect, ICSS2015 Conference

Paul Timmers from DG Connect describes the EU approach to cyber security, especially the EU's Cybersecurity Strategy from a slightly different angle as portrayed in Figure 3.7. Timmers argued, at the ICSS2015 Conference, that the three main drivers of the strategy (cyber resilience, reduction of cybercrime and cyber defence) are led by the Digital Agenda for Europe, DG Home and the EU Foreign and Security Policy (Timmers, 2015).

At a regional level the EU follows two main policies. The first is related to cybercrime, while the second is focused on Critical Infrastructure Protection (CIP), Critical Information Infrastructure Protection (CIIP) and Network and Information Security (NIS) (EU Parliament, 2011: 24; Nagyfejeo, 2012: 12). Critical infrastructures include 'facilities such as water, electricity and energy, the disruption of which would have a deleterious effect upon individuals and national security' (Nagyfejeo, 2012: 34). Critical Information Infrastructure Protection (CIIP) relates more precisely to the stability of crucial ICT structures (Nickolov 2005: 108). According to Anabela Gago (head of the unit "Organised Crime", DG Home) the EU has not reduced cybercrime directly, but helped its members to address these issues more effectively. The focus has been on strong and effective legislation, reinforcing the capabilities of Member States, and enhancing cooperation with other communities such as law enforcement (Forum Europe, 2014).

At the legislative level, the EU introduced several measures against cyber attacks, including the *2013 Directive on Attacks Against Information Systems*, which replaces the 2005 Council Framework Decision (Official Journal of the European Union 2014). The Directive attempts to avoid over-criminalisation by creating a balanced approach through the introduction of minimum standards in the definitions of online criminal offences and sanctions for those found guilty (EPRS, 2014: 2).



[Figure 3.8.]: *Legislative actions – EU response to cybercrime*

Borrowed from DG Home website, www.ec.europa.eu

These policy steps, which have been taken in order to remedy the problem of cybercrime, commenced in 2001 (See figure, 3.8, above), however the EU modernised its cybercrime laws in 2013 with the New Directive that replaces the 2005 EU Directive 2005/222/JHA. In contrast, the U.S. has not modernized the Computer Fraud and Abuse Act of 1986 (18 U.S.C. § 1030). EC3 and Eurojust have been playing a vital role in addressing cybercrime, and this will be elaborated on later in this chapter.

Infrastructure protection has been at the heart of EU initiatives over the last decade. In 2004, the Commission adopted the "Communication on Critical Infrastructure Protection in the Fight against Terrorism" (European Commission, 2006), which

suggested ‘measures to improve European defence and prevent terrorist attacks’ (Nagyfejeo, 2015: 160). The European Programme for Critical Infrastructure Protection (EPCIP) was approved in the same year and established a Critical Infrastructure Warning Information Network (CIWIN) (Bures, 2013: 77; Nagyfejeo, 2015: 160).

In 2009, the Commission adopted the ‘Communication on Critical Information Infrastructure Protection – Protecting Europe from Large Scale Cyberattacks and Cyber disruptions: Enhancing Preparedness, Security and Resilience’, which is based on five themes: ‘preparedness and prevention; detection and response; mitigation and recovery; international cooperation; and the establishment of criteria for European Critical Infrastructures in the field of ICT’ (European Commission, 2009: 149; Nagyfejeo, 2015: 160). The Digital Agenda for Europe, a part of ‘EUROPE 2020 – A Strategy for Smart, Sustainable and Inclusive Growth’, seeks to maximise the potential of ICT (Nagyfejeo, 2015: 160). In order to establish a pan-European network of national Computer Emergency Response Teams (CERTs) by 2012, it called for the establishment of an EU-based CERT, as well as calling upon Member States to set up their own national CERTs (European Commission 2010d). However, the Commission has been keen to emphasise that the challenges ahead are ‘neither specific to the European Union, nor can they be overcome by the EU on its own’ (Nagyfejeo, 2015: 160).

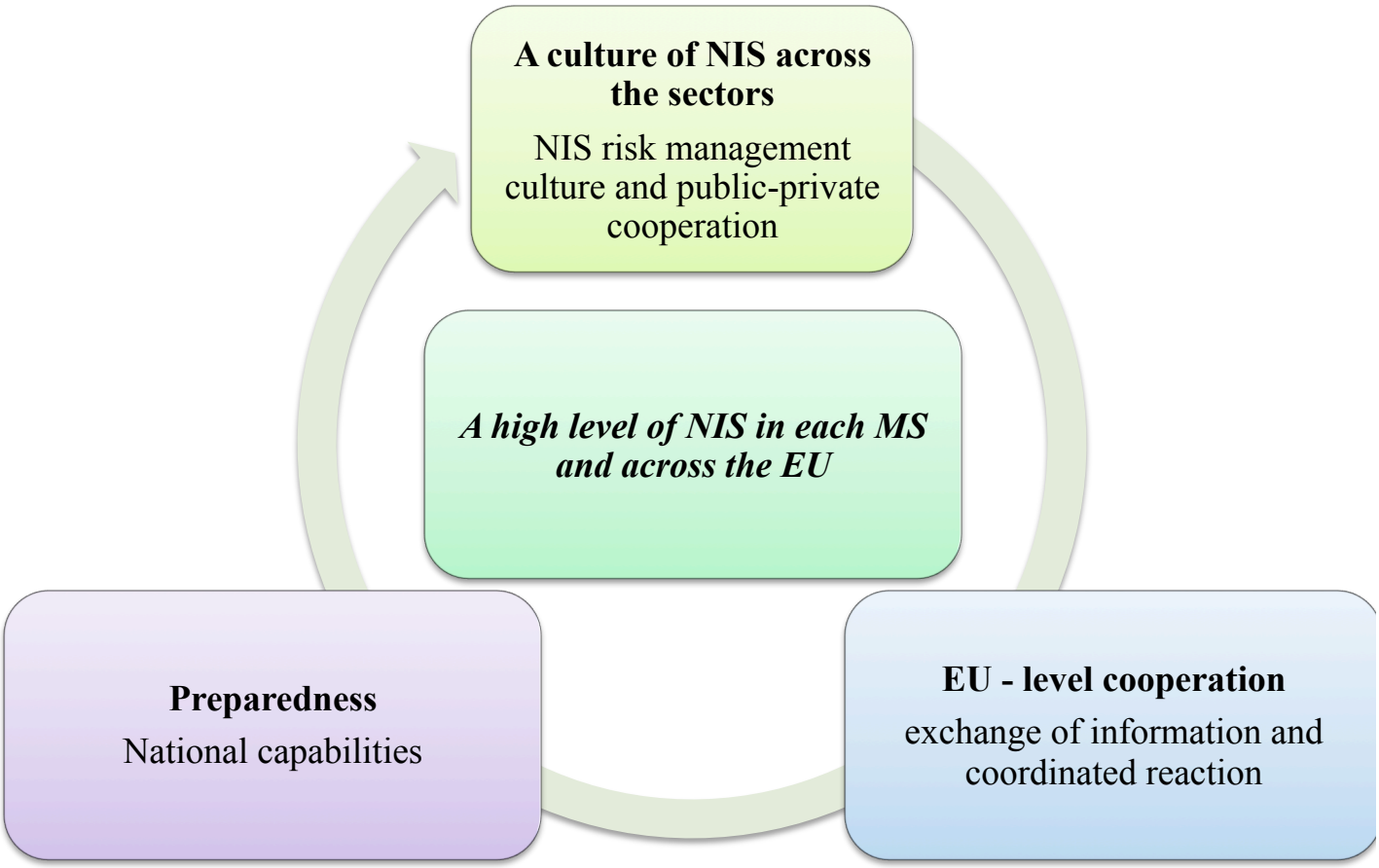
Furthermore, in May 2015 the Digital Single Market (DGM) strategy was set to be delivered by the end of 2016, with the aim of breaking down the regulatory barriers of the 28 nations in order to create a single market (EU Commission, 2016). This would

create greater access to digital goods; a safe environment to practice and it would boost the digital economy (EU Commission, 2016). Although DGM's objective might appear difficult to accomplish, it also raises the question of whether it could give the EU the lead in information and communication technology over other countries, including the U.S. (Harding, 2015).

In February 2013, the European Commission put forward its 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 – the 'NIS Directive'. This accompanied an *EU Cybersecurity Strategy* based on core peaceful, democratic, European values (European Commission, 2013a: 1, 4). These measures focus on the enhancement of cyber resilience by creating a system for the reporting of security incidents. This "regulatory" incident reporting scheme can be regarded as a crucial step in enhancing the protection of CIs. The main goal is to apply it not only to service providers such as providers of healthcare, energy, transportation and financial services, but also to market operators in the "internet economy" more generally (EU Parliament, 2013). The NIS Directive experienced a mixed reception from various stakeholders mostly because the term 'market operators' was ill-defined, for instance it is unclear whether social media companies like Facebook are obliged to report under the requirement (EU Commission, 2013c).

The NIS Directive, which aims to improve pan-European coordination on cyber security incidents, also contains a mandatory notification obligation. However, it is related to incidents that do not necessarily have to include the disclosure of data, although there may be an overlap with the GDPR where a security incident also

involves a personal data breach. Nevertheless, the two pieces of legislation are designed to address different subjects (Boué, 2015). One of the reasons for the introduction of the NIS Directive is the lack of a pan-European cyber security law since incident reporting is currently only applied rigorously to telecoms operators. In the NIS directive, the market operators, who are subject to the directive, will have to notify the competent authority (this new NIS authority has to be established by each Member State) in case a cyber security incident occurs. In practice, a cyber security incident and a data breach will quite often happen in parallel, however, in the case of the NIS Directive, there is no notification deadline specified.



[Figure 3.9.]: *Three Pillars of Network and Information Security (NIS) Directive*

Source: Derived from Paul Timmers, DG Connect, ICSS2015 Conference

The NIS Directive requires EU Member States to adopt national NIS strategies and plans for cooperation on cyber-security, together with the creation of a civilian competent authority (CA) alongside the national CERTs. It is envisaged that the CAs will play a crucial role in a pan-European secure communications network, helping to facilitate the smooth sharing and exchange of cyber security-related information (including incident reports) (European Commission 2013c; EU Parliament 2013). The implication is clearly that smaller national governments are being encouraged to direct more resources to their national technical authorities and thus catch up with leading states.

In March 2014, the European Parliament adopted the proposed Directive, and the new legislature, and then had the task of coming to an agreement with the Council on the final text. It is hoped that the NIS Directive should at least address some of the current concerns about cyber attacks while calling for minimum standards. It will obviously also increase the resilience of the system, although it will admittedly create an administrative burden for small SMEs. There is also an interesting parallel with the NIST framework within the U.S. that has been making some progress recently. NIST standards were on the agenda of the EU–U.S. ministerial meeting in Athens on 25th June 2014.

Remarkably, it was not until December 2015 that the EU Council and the EU Parliament came to an informal agreement on the NIS Directive. This was formally adopted by the Council in May 2016 (EU Council, 2016) and is regarded as 'the first set of cyber security rules for operators of essential services and digital service providers' (Council of the EU, 2015). As former EU Commissioner for the Digital

Agenda, Neelie Kroes, stated, the NIS Directive aims to 'reduce fragmentation caused by 28 different markets, 28 rulebooks, 28 referees and 28 mind-sets' (Van Eecke and Marshall, 2015). Once it is formally adopted, Member States will have 21 months to implement it. One of the criticisms, however, levelled by the law enforcement (LE) community, is that there is no obligation for notification of the law enforcement authorities (Interview, 2015d).

Discussion of the NIS Directive began in 2013, but it took almost three years for the EU to reach an informal agreement. While this was slow, it nevertheless demonstrated that the EU has a strong regulatory-legal cyber culture (rather than a military culture) that advocates a regulatory approach in order to enhance resilience, boost the Digital Single Market and reduce differences across the national cyber cultures of the 28 Member States. The advantage of this directive over a regulation is that it takes into account the various cultural and social differences that are present among the EU Member States. It therefore provides sufficient space for each Member State to use their own means and methods of implementation and alignment of the directive's requirements within their own national law.

Nevertheless, the NIS Directive remains controversial and has been delayed because of disagreements among the Member States on the definition of the types of companies that need to be included within the scope of the reporting. Again, this demonstrates the lack of unity from the EU as Member States have different priorities, often driven in turn by divergent market/economic interests that cannot be disregarded easily. We can broadly disaggregate states into two groups:

(1) The first group includes Member States, which host U.S.-based Internet giants (e.g. Amazon, Google, Cisco, and Facebook) and consequently, prefer to minimise the involvement of such 'over-the-top' companies within the scope of the Directive.

(2) The second group includes Germany, France and Spain who prefer these 'over-the-top' companies to be included within the scope of the Directive and obliged to make reports in respect of cyber incidents (Fleming, April 2015).

Another dispute that arose between EU lawmakers and Member States regarding the NIS Directive can be linked to what types of digital platforms (search engines, social networks, e-commerce sites and cloud computing providers) should be included within the scope of the Directive (EurActive, 2015b). Since the negotiations have been on-going since the summer of 2015, those firms that meet the legal definition of digital service platforms will also be included now within the scope of the Directive with lighter security obligations even though the European Parliament would prefer to limit the scope to the truly essential critical infrastructure such as energy, transport and finance (Walker, 2015). To what extent online services will be treated differently in terms of cyber breach notification obligations and how it will be put into practice still remains a controversial issue (Interview, 2015e).

3. Legal-regulatory dimension of EU strategic cyber culture

This section seeks to demonstrate that EU strategic culture displays stronger legal and economic aspects, set against military aspects, and furthermore, that this is also reflected in detail at the level of EU strategic cyber culture. In other words, the empirical research conducted for this thesis strongly suggests that EU strategic cyber

culture has a much stronger legal-regulatory dynamic when compared with military systems. This explains why the EU is focused more on the civilian aspects of cyber security and it is therefore essential to examine the way this strong legal–regulatory culture is manifested in the EU approach to cybercrime.

To repeat, the concept of strategic culture needs to be extended beyond the scope of the military and defence, since cyber security, especially within the EU context, is not limited solely to the 'use of force' but also encompasses the fields of economy, trade (digital economy) and diplomacy/foreign policy. The trans-institutional nature of cyber security does generate overlaps and intra-governmental communication problems as there are many EU institutions working on various cyber security tasks. Therefore, it is important to understand how coordination within the EU cyber security policy puzzle works in order to put the various elements together and gain a clearer picture of the various tasks.

It is most important to emphasise that EU cyber security policy strongly reflects the institutional culture of the EU. This assists in explaining why the EU has a predominantly legal and political culture. *The Single European Act* of 1987 and the *Maastricht Treaty* of 1992 were crucial in terms of laying down the economic and legal foundations and creating what Shore suggests has developed into a nascent 'European State' or, in other words, according to Goldstein 'the first transnational state of the nuclear era' (Shore, 2001; Goldstein, 1993: 122-3). By contrast, other scholars, such as Hoffman, argue that, unlike nation states, the EU is still lacking a common culture around which 'European consciousness' could emerge to support the economic and legal foundations (Hoffman, 1993: 31).

Back in 1995, Jacques Santer's first speech to the European Parliament as Commission President emphasized that 'the future of the Community can no longer remain the prerogative of a select band of insiders' (Santer, 1995: 4; Shore, 2000:19). This critical evaluation was also shared by other scholars like Hoffman, arguing that European integration is still an 'elite-driven, technocratic affair orchestrated primarily by a small layer of key politicians and civil servants' who have little connection with the European citizens who are essentially the main pillars for the EU's existence (Hoffman, 1995: 235; Shore, 2000).

This view is also supported by the '**second generation**' of strategic culture theorists - Bradley S. Klein and Robin Luckham – who argue that in reality the selfishness of a small hegemonic community drives strategic choices instead of the wider strategic culture (Sondhaus, 2006: 8; Klein, 1988; Luckham, 1984). Their suggestion is that the elite have the power to distort strategic culture in a Machiavellian way when strategic decisions are made, which implies that there is a difference between the ways they claim to act and what they are actually doing in reality (Poore, 2003: 284). But twenty years on from Santer's famous speech - has this situation changed at all? Partially, the answer is "yes", in some fields. And what is the story with EU cyber security? Are EU cyber security strategic decisions shaped by the masses or the elite? The answer is probably "both", working in partnership. Before a more detailed answer can be given to these questions, the institutional context must be considered.

During the 1980s, international scholars began to explore the complex environments in which global governance occurs and to study the institutions that facilitate regional

collaboration (Kransner, 1983; Keohane, 1984; Young, 1988; Powell and DiMaggio, 1991: 6). International regimes of governance – like the EU – could be understood as 'multilateral agreements, at once resulting from and facilitating cooperative behaviour, by means of which states regulate their relations with one another within a particular area' (Powell and DiMaggio, 1991). In short, it is possible to conceive of regimes as institutions that assist with stabilising international order whilst normalising and producing standard expectations (Powell and DiMaggio, 1991). Keohane, while accepting this broad contention, added the important qualification that 'it leaves open the issue of what kinds of institutions will develop, to whose benefit, and how effective they will be' (Keohane, 1988: 388). The European Cybercrime Centre (EC3) was created in 2013 to make EU citizens and businesses safer by facilitating faster reactions to online crimes and the ENISA was created in 2004 to provide reliable information and advice on information assurance to all parts of the EU. These are the two institutions that are most pertinent (Lloyd, 2014: 200-201).

However, the different settings in which the stakeholders of EU Member States are operating also need to be considered. In this sense, it is in the best interest of all Member States that their information assurance systems are developed in a 'cooperative manner and cyber security therefore needs to be managed in an integrative form' (Nagyfejeo, 2012: 41). In this respect, the focus of many of the European countries has been to 'facilitate common *standards and protocols* (for example, ETSI), which can be developed to guarantee the improvements that address threats to cyber security' (Nagyfejeo, 2012: 41). One possibility is to ensure that EU

institutions have a mandate to coordinate the different European opinions, and the efforts of European organisations to ensure the maximum strategic convergence.

There is clearly insufficient space within this chapter to examine the different approaches and theories concerning European institutions generally. However, it might be worth noting the approach represented by sociological institutionalists, which is one of the dominant interpretations of the wider EU cultural dynamic. These scholars maintain that culture is an important element within EU frameworks. They argue that cultural and historical frameworks cannot be ignored when individual choices and preferences are made. More precisely, people living in different societies (EU Member States) or even institutional domains (for example, EC3, EDA, DG Home) maintain different norms about the interests that motivate legitimate action at various times (Powell and DiMaggio, 1991). Furthermore, both 'old' and 'new' institutionalism share an emphasis on the importance of the correlation between organisations and environment, and therefore prioritises the role of culture in 'shaping organisational reality' (Powell and DiMaggio, 1991:12). A specific example of this is the existence of a common legal environment, like the one existing within the EU, which shapes many features of the EU's behaviour and structure (Powell and DiMaggio, 1991: 67).

3.1. New modes of EU decision-making: a strong legal culture?

Some important institutional changes have occurred regarding the EU ordinary legislative procedure (OLP), particularly concerning the right of initiative since the Lisbon Treaty (2007), which enhanced the Maastricht Treaty (1993). Since the Lisbon Treaty came into effect on 1st December 2009, the EU Parliament has earned the

'secondary' right of legislative initiative that authorises the Parliament to ask the Commission to submit a proposal (Diedrichs *et al*., 2011). This is a major departure from the 1957 Treaty of Rome, which only authorised the EU Parliament to take an advisory role in the legislative process, whilst the Commission enjoyed the 'exclusive right of initiative', and the Council adopted the legislation. In other words, as a result of the Single European Act (1986) and the Maastricht, Amsterdam, Nice and Lisbon Treaties, the EU Parliament's participation has been notably strengthened by extending the OLP to new policy areas. The materialization of bicameral legislation (co-legislation) comprising of the Council and the EU Parliament has thus been witnessed (Diedrichs *et al*., 2011: 217).

These observations about changes to the ordinary legislative procedures, while general, are nevertheless valuable as they support gaining a clearer picture regarding the way EU Cybersecurity Strategy and the Commission's Network and Information Security (NIS) Directive have been developed. However, attention needs to be given, first and foremost, to the field of 'Justice and Home Affairs', which plays an increasingly important role in developing legislation on EU cyber security, especially in the fight against cybercrime. Moreover, this area provides further evidence of the legal and regulatory strengths of EU strategic culture in the area of cyber security.

The developments in the field of Justice and Home Affairs could be divided into five main 'eras' (Bunyan, 2013):

- Trevi era (1975-1993)
- Schengen era (1985-1999)
- Maastricht Treaty era (1993-1999)
- Amsterdam Treaty era (1999-2009)

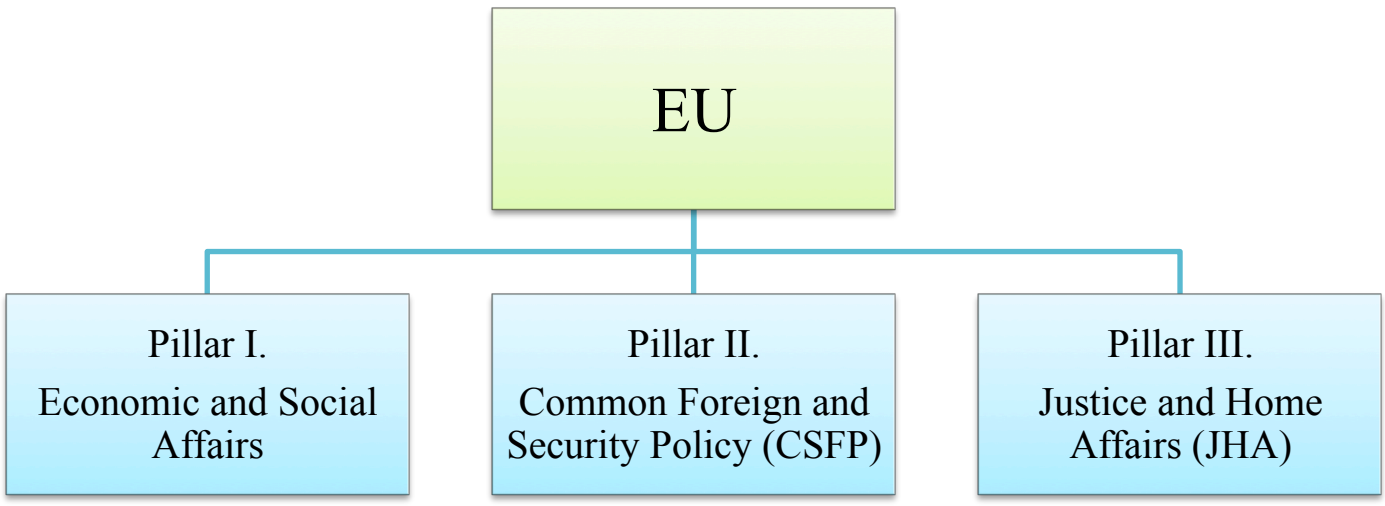
- Lisbon Treaty era (2009 - ongoing)

During the 1970s, there was a tremendous increase in the number of terrorist attacks across Europe, many of which were carried out by domestic terrorists with an ideological or separatist agenda. Based on statistical data, the number of terrorist incidents in Europe in the 1970s was 3,498 with 8,114 worldwide (Russel, 1979: 158; Hampton, 2013). For example, attacks were carried out in Spain by the Basques, in Germany by the RAF, in Italy by the neo-fascists, in Great Britain by the IRA, and in France by the Algerian separatists, to mention only a few active organisations. This marked an important moment in the crystallisation of EU security culture, since almost all European governments favoured a civil approach that involved emphasising the rule of law to *criminalise* the terrorists. Hampton argues that the European *law and order approach* was a determinant factor in the early development of European strategic culture where the 'nature of threat is defined in terms of rational problem solving, therefore calling for a rational response' (Hampton, 2013: 121). Europe treated terrorists as criminals, in contrast to the U.S. where they were deemed to be 'evildoers'. Europeans therefore preferred to advance middle-of-the-road law and order responses against the terrorist attacks as these were seen as a domestic threat to social cohesion. Despite differences in terrorism from one state to the next, the majority of governments focused their efforts on boosting their police techniques, surveillance, intelligence gathering capabilities and paramilitary skills, together with enforcing existing legislation better, in order to respond more effectively.

In 1999, the Treaty of Amsterdam came into effect and helped to develop the EU as 'an area of freedom, security and justice' (AFSJ), although this did not "supranationalise" the policy area. The main goal of this new development, according

to Kaunert, was to weaken the power of full national sovereignty by providing 'limited mandates and weak institutional instruments and structures' (Kaunert *et al.*, 2012: 9). Consequently, the JHA domain's expansionist behaviour became manifested in its presence in other policy areas, such as the EU's external relations and the internal market. While some issues, such as the asylum and visa policy, were shifted to the First pillar, others remained under the Third pillar, namely police and judicial cooperation on criminal matters and the maintenance of an effective collaboration between the competent judicial and law enforcement authorities of the Member States.

Furthermore, the normative trend to treat the AFSJ independently from the Single Market was reinforced by the Lisbon Treaty that came into force on 1st December 2009, bringing further significant changes in its wake: (1) the abolition of the three pillar system; (2) the EU Parliament was empowered with equal status over policing and judicial cooperation on criminal law; (3) the procedure of 'co-decision' between the Council and the Parliament was renamed and became 'ordinary legislative procedure' (Bunyan, 2013: 3).



[Figure 3.10.]: *"Old" Pillars of the EU before the Lisbon Treaty entered into force in 2009*

Nevertheless, the functioning of the JHA is not without problems. The JHA approach to cooperation can be viewed as one of the core challenges, as the application of law enforcement is strictly limited to national authorities; in other words, *state sovereignty* remains a disturbing problem (Diedrichs *et al*., 2011: 181). This becomes an even more perplexing issue in connection with the prosecution of cybercrimes, an intrinsically transnational form of crime that does not respect the sovereignty of nation-states, therefore causing several complex legal problems in the JHA domain.

Considered from this perspective, it becomes easier to see why the EU represents, at its core, a strong legal and regulatory culture that shapes the way EU policies are formed and created within the JHA domain. Logically, it could be assumed that EU policies in the field of cyber security, especially on cybercrime, are following a similar *regulatory path*, in other words, *law and crime approach*, to other issues in the JHA domain. This also indicates why EU strategic culture has been 'slippery' in the defence context but more coherent in the cybercrime context. It might be added that the latter is widely believed to be the most developed and successful cyber cooperation platform between the EU and U.S.

3.2. DG Home: fighting cybercrime in partnership with the U.S.

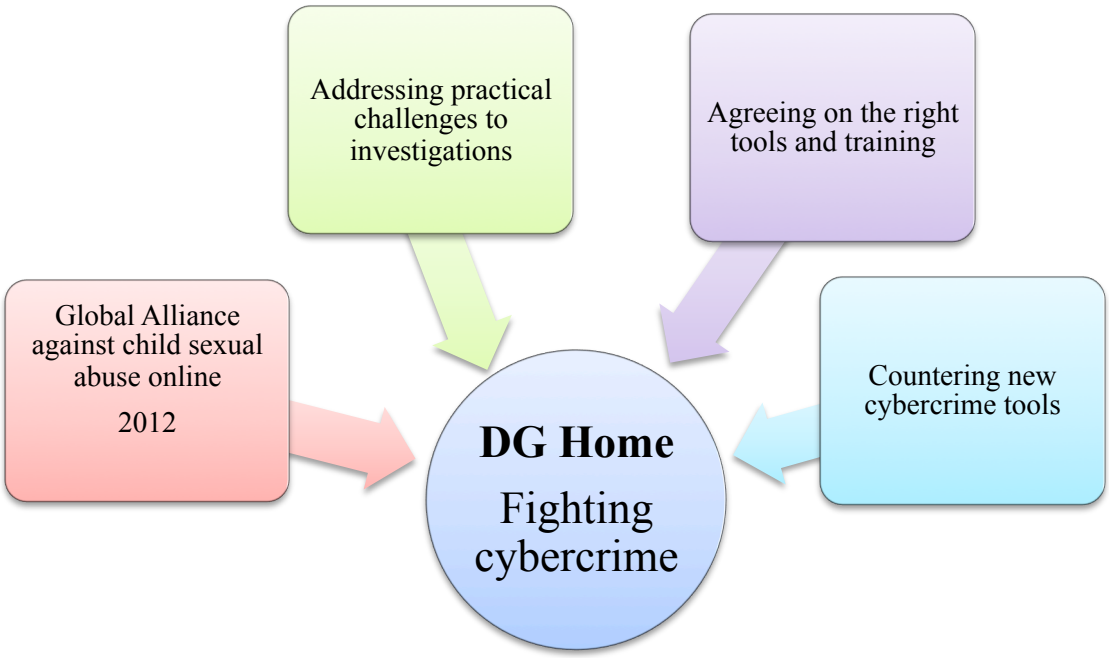
Whilst *DG Connect* has been responsible for promoting cyber incident management, public-private partnerships and public awareness, *DG Home* has taken the lead on tackling cybercrime, focusing on four main areas:

(1) Global Alliance against child sexual abuse online

(2) Addressing practical challenges to trans-border cybercrime investigations – improve the approach to investigation and prosecution and sharing of best practices

(3) Agreeing on the right tools and training for domestic cyber law enforcement agents

(4) Countering cause for new cybercrime instruments



[Figure 3.11.]: *DG Home fighting cybercrime*

(1) Global Alliance against child sexual abuse online

In December 2012, former Commissioner Malmström and U.S. Attorney General Eric Holder launched the *Global Alliance against Child Sexual Abuse Online,* widely considered to be the most successful platform in the EU–U.S. cyber dialogue (EEAS, 2014). The success of the platform is shown by the voluntary enrolment in this political initiative by 54 countries who have made a commitment to strengthening five core issues in their national framework: (1) diminish child sexual abuse online; (2)

protect and support victims; (3) moderate the accessibility of child pornography online; (4) prosecute offenders; (4) promote public awareness (EEAS, 2014).

This global alliance is a clear demonstration that shared interests and views on certain issues can foster meaningful collaboration, even between actors coming from different cultural backgrounds. Specifying common interests and threats – since most international actors do *not* support child abuse and paedophilia online – can foster trust among various stakeholders by creating functional alignments that are operationally effective across jurisdictions. For example, in March 2014 the U.S. Department of Justice prosecuted a U.S. citizen and imposed a 30-year sentence because he was working as an English teacher in China and taking advantage of that situation to molest children and take pornographic photos (Dep. of Justice, 2014a). Transparency, effective information sharing and the establishment of a Pan-European or global based framework (that is both regionally managed and centrally located) would be a significant step towards the prosecution of cybercriminals. A key requirement is that this consensual framework is adhered to by every stakeholder, regardless of cultural and educational background.

Similarly, the Global Alliance against Child Sexual Abuse Online has four potential policy targets to which everyone readily subscribes:

a) Improving victim identification and assistance
b) Improving investigation and prosecution
c) Raising awareness
d) Reducing the amount of child sexual abuse material online

(Interview, 2014f).

Until 2014 the Commission was acting as the Secretariat of the Alliance, then this role was handed over to the U.S. Ministry of Justice contacts under Attorney General Holder (Interview, 2014f). DG Home is responsible for reporting, and has thus created a website which all 54 countries now use to send reports to DG Home on actions undertaken relating to the protection of children online (DG Home, 2015). In addition, a Second Ministerial Conference of the Global Alliance against Child Sexual Abuse Online was held in Washington DC in September 2014 which aimed to expand the alliance and promote the four policy targets. It also acknowledged the fact that there is still not sufficient access to information and shared evidence among law enforcement organisations operating in different countries (DG Home, 2014).

(2) Addressing practical challenges to trans-border cybercrime investigations

The "main customer" of DG Home is considered to be law enforcement, and the issue of cybercrime jurisdiction is a very real challenge in this area (Interview, 2014f). One example of this challenge is a cybercriminal living in Belgium who hacks into an account in France and steals some sensitive information (password and bank details) but the servers are housed in the U.S. when the crime is taking place. This prompts the question: which jurisdiction does the crime fall within? There have been a number of discussions addressing these complicated issues, and they have focused on what might be termed "hot pursuit" and relates to the U.S. provisions for obtaining data rapidly in an emergency and the requirement for a Mutual Legal Assistance Treaty[7] (MLAT) (Interview, 2014f).

[7] MLAT is a treaty-based mechanism for seeking foreign law enforcement cooperation and assistance in support of an ongoing criminal investigation or proceeding.

Requests under MLAT are considered to be 'faster and more reliable than letters rogatory'[8] (Brenner, 2010: 143). The difference between MLATs and letters rogatory is that MLATs are 'designed to work quicker since the MLATs impose an international legal obligation on the requested state to respond, whereas letters rogatory can only request a response' (Brenner, 2010: 143). From the U.S. perspective, the first step an officer who requires evidence from abroad must undertake is to establish, through the Department of Justice's Office of International Affairs (OIA), whether an MLAT exists with the country where that evidence is (Federal Judicial Center, 2014: 7).

In the EU, the Maastricht Treaty (1993) under Title V. declared a common internal security space forming the JHA pillar which introduced judicial cooperation in criminal matters that follows the principle of mutual acknowledgment of the judgements and decision by EU countries (Marsh & Rees, 2012: 20). However, the post-Lisbon era has revolutionised JHA law, and so the EU has been granted a 'single legal personality' and competences to regulate the criminal law, functioning as a new legal background in accordance with Article 82 TFEU and Article 83 TFEU (Herlin-Karnell, 2012; Fahey, 2014: 20).

To illustrate this new development, when a cybercrime takes place this is often followed by an urgent request from a Member State for information from a foreign online service provider (often based in the U.S.), and the requirement to access digital evidence relating to the cybercriminal. Depending on whether the data request is content based or not, the appropriate legal procedure has to be followed. For instance,

[8] Letters rogatory are requests from judges in the United States to judicial officers in foreign countries for assistance.

non-content data requests typically do not need the MLAT process but content-based exchange of information does (Interview, 2015f). However, MLATs are still remarkably slow procedures that can take up a year or more to process. Both letter rogatories and MLATs are, therefore, not very practical when it comes to the investigation and prosecution of cybercriminals, since there is every risk that the digital proof the officer would like to obtain will be 'deleted before his request even reaches the appropriate foreign authorities' (Interview, 2014f; Brenner, 2010: 143). Therefore, there is a clear need for MLAT process streamlining and to create a universal arrangement that could be applied to cybercrime terminology (EU Council, 2015a). A further limitation to law enforcement cooperation and access to information abroad is provided by cloud computing, particularly as cloud storage can mean that data is located in a variety of different physical locations and these may have conflicting legal frameworks.

(3) Agreeing on the right tools and training for domestic cyber law enforcement agents

Another significant programme funded by DG Home is The Prevention of and Fight against Crime (ISEC), which aims to provide security for EU citizens whilst combatting problems such as cybercrime. It had a budget of EUR 600 million for the period 2007–2013 it, yet many observers still considered this to be a small resource compared to Horizon2020[9] (Interview, 2014f). Similarly, in the last seven years the Commission has set up the European Cybercrime Training and Education Group (E.C.T.E.G.), which basically brings together all the 28 Member States representatives' training and academic specialists. E.C.T.E.G. sets up various courses

[9] Horizon2020 is the biggest EU Research and Innovation programme ever with nearly €80 billion of funding available over 7 years (2014 to 2020).

and curriculums specifically tailored to law enforcement in cybercrime investigations (ICSS2015 Conference).

(4) Countering cause for new cybercrime instruments

The Convention on Cybercrime (also known as the Budapest Convention) is widely regarded as the first international treaty that attempts to harmonise national criminal laws and criminal prosecutions in order to tackle crimes committed online (Council of Europe 2001, No. 185). According to Bendiek, one of the obstacles to effective legal protection is the lack of standard definitions of what kind of criminal acts online should be punished by law. What complicates this even further is the absence of an agreement on whether information about suspected criminals can or cannot be shared (Bendiek 2014: 7). In those countries that have not ratified mutual legal assistance treaties, or where the criminal attacks performed online are not a breach of that country's national criminal law, it is very easy for extremists (such as terrorists) to set up terrorist sites as private forums. The Convention that came into effect in 2004 aims to close this legal loopholes by setting up common standards that help to establish whether an online crime has been committed (Bendiek 2014). This treaty might well be considered a pathfinder towards a common judicial area in which to fight online crime effectively.

The Budapest Convention has not secured thorough harmonisation. Different cultural values can still pose obstacles when it comes to fighting cybercrime. The introduction of a legal requirement for mandatory data retention is an example of an area, which is making it difficult for some of the European signatories to implement the conditions

of the Convention (Yannakogeorgos and Lowther 2013: 253). Another critical point is that the Convention requires the criminalisation of racist propaganda, even though in some countries (e.g., the U.S., Brazil, China and Russia) such a ban would be considered as an infringement of national legal principles or violation of the freedom of expression (Bendiek 2014).

EU officials repeatedly emphasise that the Budapest Convention is the necessary basic framework for setting up legislation in the fight against cybercrime. In other words, it is widely agreed in the EU that there is *no need* for new laws or specific treaties and instead it can largely rely on existing laws (Forum Europe, March 2014). The EU is therefore opposed to the position of the BRIC countries (Brazil, Russia, India, China, and South Africa) who support the concept of a new UN treaty on cyber security. It is felt that this treaty could change governments' power of enforcement of human rights online, for example, arresting aggressive Chinese bloggers who try to challenge the Chinese government propaganda by spreading rumours (Interview, 2014f). This demonstrates that a strategic cyber culture driven by China would provide different interpretations and applications of rules and laws, and this would create a less secure ecosystem.

3.3. Eurojust and its role in fighting cybercrime

Eurojust was set up in 2002 acting as the judicial branch of EU law enforcement in the fight against serious crime (EU Council, 2002). As an EU agency it plays a vital role in providing legal assistance in cross-border investigations especially concerning the application of the MLATs and extradition requests (Eurojust, 2015). Additionally, Eurojust works closely with other agencies like Europol, the European Anti-Fraud

Office (OLAF) and European Judicial Network (EJN) and the contact points of 23 other non-Member States (Van der Meulen et al., 2015: 55).

Furthermore, Eurojust assists national cybercrime investigations and prosecutions in order to speed up information sharing on legal matters (Hayes *et al*., 2015: 29). Other tasks it is involved in include assisting with the identification of requirements for the cybercrime Training Competency Framework, and providing materials as well as trainers, but it has no leading or governance role. Eurojust has also recently become the observer member in the J-CAT Board (Interview, 2015g). The European Cybercrime Task Force (EUCTF), which was created in 2010, is also funded by Eurojust (Dinkwater, 2014). It is considered to be a high-level platform that is made up of the head of national cybercrime units, EC3, Eurojust and the Commission and it aims to share best practices and synchronise the EU actions against cybercrime (Van der Meulen et al., 2015: 55).

Eurojust, acting as the legal carrier of EU strategic cyber culture, further suggests that the application of strategic culture in cyberspace is not limited solely to the use of force and defence. Still, the legal dimension is considered to be the most challenging aspect related to international cybercrime investigations.

Furthermore, in November 2015 Eurojust and EC3 put together a joint paper that addressed common practical and legal challenges faced when combating cybercrime (EU Council, 2015a). The following obstacles have been identified: 1) loss of data and location 2) legal framework 3) public-private partnerships 4) international cooperation and 5) evolving threat landscape and the expertise gap (EU Council,

2015a). Based on the interviews conducted with senior cybercrime prosecutors from both the EU and the U.S., the areas that have resulted in the most complaints have been the legal framework and the collaboration with the private sector. The legal framework is problematic because of the differences of domestic laws, criminalisation conduct, cybercrime investigation facilities and e-evidence gathering (EU Council, 2015a). In addition, there is no international legal framework that would advance evidence sharing (EU Council, 2015a).

The major obstacles encountered in collaboration with the private sector have been concerns relating to liability and data protection regulation and these are connected to the fear of loss of reputation. The extent to which law enforcement, jointly with prosecutors, can establish equally trusted partnerships with private industries which are simultaneously in competition with each other, has always been questionable. Collaboration at the EU level is also hampered by the differences of domestic laws among Member States, because not every Member State has the legal basis to authorise national law enforcement to directly appeal or subpoena a foreign ISP, and the only legal instrument they rely on is the cumbersome MLAT process (EU Council, 2015a).

4. Operational dimension of EU strategic cyber culture: EC3

According to Bures, one of the EU's key counterterrorism instruments is Europol, which was initiated by the Maastricht Treaty and started to function in a limited way as the Europol Drug Unit (EDU) in 1994 (Council of the European Union, 1999). Europol acted as the EU's police unit and became fully operational in 1999 when all Member States finally ratified the Europol Convention (Bures, 2006: 59). Its scope

was extended gradually to deal with 'crimes committed or likely to be committed in the course of terrorist activities against life, limb, personal freedom or property' (Council of the European Union, 1999). Bures argues that Europol's efficiency is greatly dependent on the willingness of Member States to share national intelligence and law enforcement information. Unfortunately, as some Member States still do not consider Europol an effective counterterrorism tool, they therefore advocate bilateral cooperation and information sharing over collective activity (Bures, 2006: 72; Bures, 2013: 65). One explanation for this behaviour lies in the diverse 'cultures of secrecy' within each Member State, which create anxiety over sharing of confidential intelligence materials in a multi-lateral environment (Bures, 2013: 72). Consequently, in the realm of terrorism, Europol remains as a mere coordination office rather than as an operational centre (Hillebrand, 2013: 102).

One of the three main challenges regarding the effectiveness of Europol lies in the various administrative, political and judicial frameworks that exist among the Member States. Furthermore, within the EU, the principle of subsidiarity allows each state to allocate which national agency is held responsible for counterterrorism. In other words, while the police might be the organisation that takes the lead on counterterrorism issues in one Member State, it is the intelligence agency in another. According to Deflem, further complexities occur when these agencies are interested in different information, for instance, the police require materials, which support an arrest and the conviction of a suspect, while the intelligence agency only needs forecasting material (Bures, 2013: 72; Deflem, 2006: 351). The third obstacle is strongly linked to the cultural and linguistic diversity that exist within the EU, for example, all essential counterterrorism related information gathered by Europol has to

be translated into all languages before it is sent out to the national agencies (Bures, 2013: 72).

The ***European Cybercrime Centre*** **(EC3)** which was established in February 2013 as part of Europol acts as a coordinator - a 'focal point' - that facilitates collaboration in the fight against cybercrime, both on an operational and strategic level, between the Member States and non-EU partners. EC3 also has no executive power and only provides a supporting role, so is thus fully dependent on the willingness of Member States and non-law enforcement partners to contribute. During cybercrime investigations, EC3 collaborates closely with Eurojust therefore becoming a collective voice of law enforcement and judicial investigators (IBP, 2014).

The EC3 mandate focuses on three main areas:

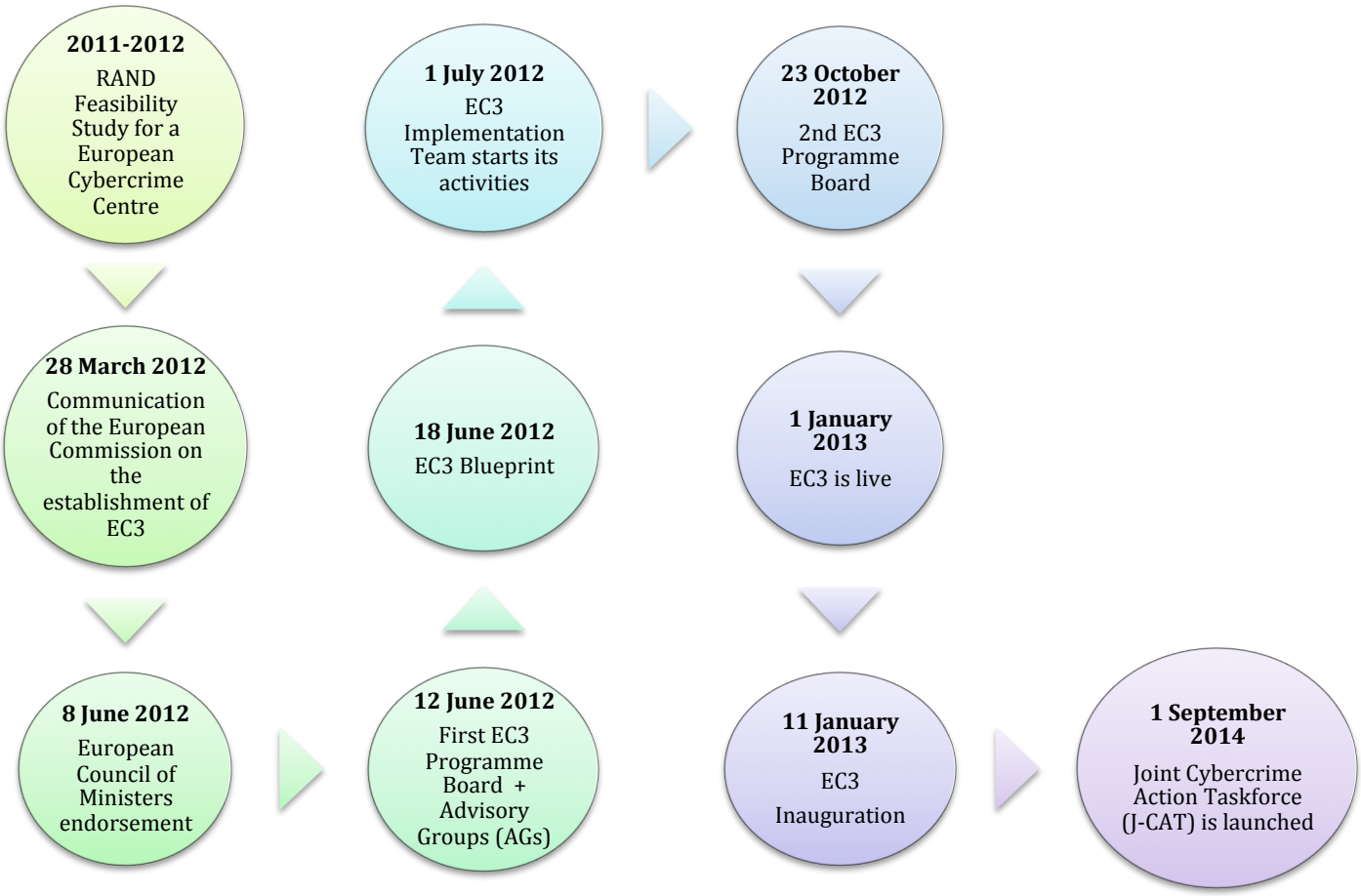
a) *FP Terminal* is in charge of assisting EU law enforcement authorities (LEAs) in a variety of cybercrime cases such as online and credit card fraud, which produce huge profits for organised criminal groups.

b) *FP Twins* is in charge of identifying cybercrimes including sexual exploitation of victims, such as children, and is responsible for creating cross-links between the participating Member States.

c) *FP Cyborg* is in charge of preventing and combating cyberattacks targeting EU critical infrastructures and information systems (for example, ICT driven organised crime aimed at financial gain) (EC3, www.europol.eu). In addition, EC3 acts not only as an intelligence focal point but also facilitates 'pooling and sharing' with Member States in cybercrime investigations.

Despite these positive steps (for example, preventative measures, joint cybercrime investigations) on the EU level, the law enforcement community and policy makers are in reality still lagging behind cybercriminals in terms of capacities and efforts to keep up-to-date with the new technologies. Year by year, the size, scope and sophistication of cyber threats and the emergence of new attack vectors are increasing and this makes the fight of law enforcement ever more difficult. The challenge is not only linked to the transnational nature of this type of crime, but it is also related to the fact that most of the relevant data and evidence are held by the private sector. In addition, attribution is another obstacle, since criminals could easily abuse encryption and anonymity services, and that makes the verification of 'who is behind a nickname or IP address' problematic. Similarly, if the evidence is physically stored in different jurisdictions then the first step is the identification of the relevant legal framework and to see whether there is an MLAT with the country that is affected by the cybercrime.

Accordingly, much time and effort is required to gather digital evidence by going through the chain of custody and establishing whether the evidence is admissible (Interview, 2015h). Consequently, the differing power capability between police and the private sector raises important issues about the governance of the internet and online police capability is an issue which must be resolved by legislators. An additional problem is that financial institutions fail to report incidences of fraud to the police, as they are afraid that this will result in a loss of reputation.

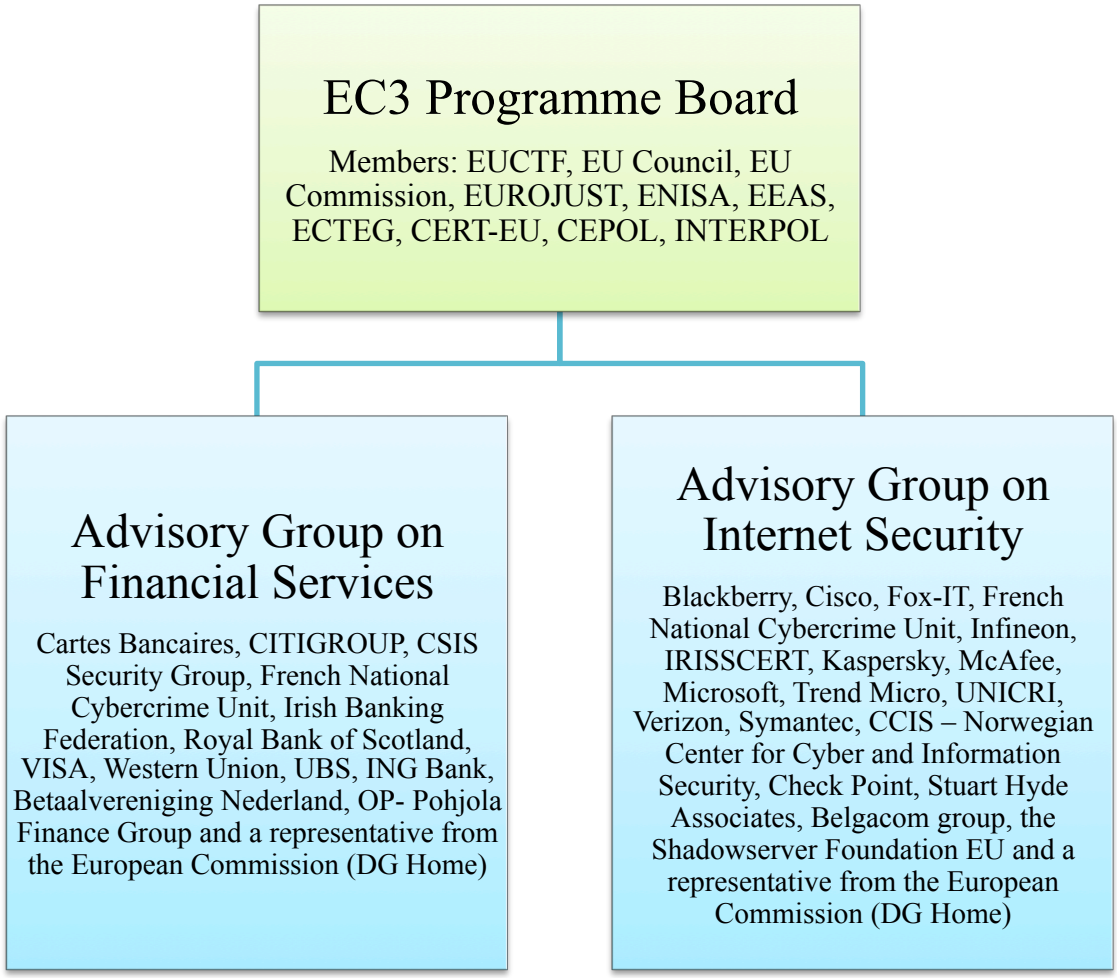


[Figure 3.12.]: *History of EC3*

Source: Borrowed from Philipp Amann, EC3

The EC3 Programme Board was created in 2012 with the aim of assisting with EC3's strategic decision-making, and two advisory groups (AGs) that are made up of non-law enforcement partners were also established: (1) AG on financial services and (2) AG on internet security (Interview, 2015h). The membership and exchange of information (not personal data) are established voluntarily and 'Law Enforcement-Private' partnerships are formed by an agreement called a Memorandum of Understanding (MoUs) that is non-binding and provides a 'formality' to the agreement. According to a senior Europol official notwithstanding that these MoUs may appear from the outside to be a positive first step, they are not very beneficial to

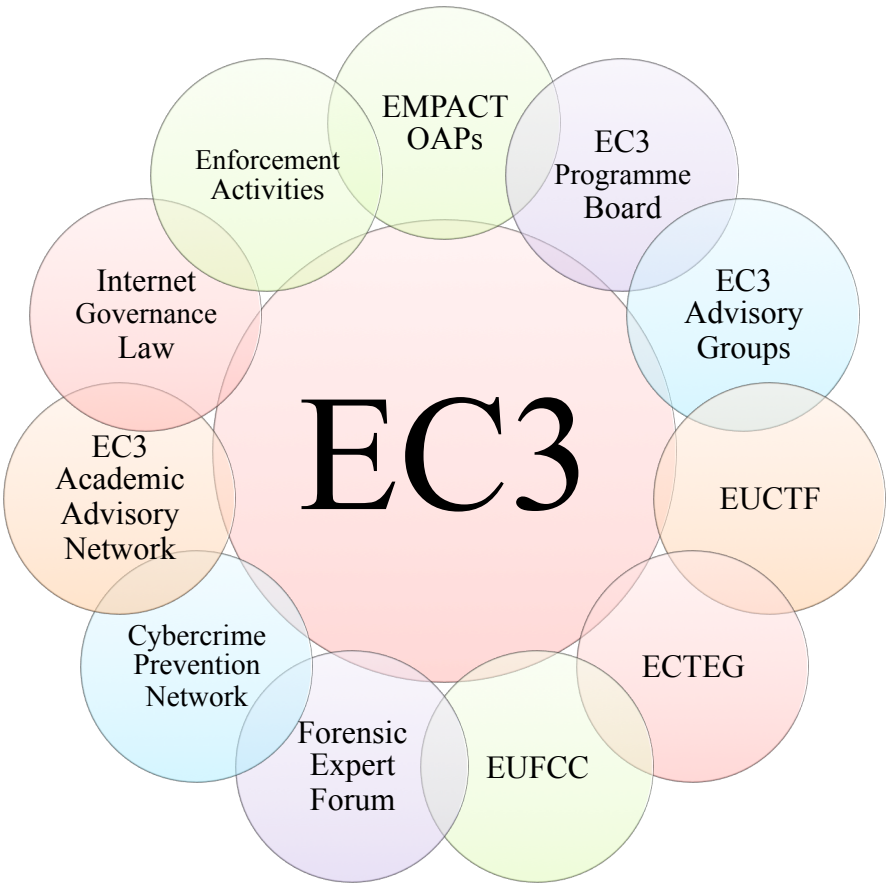
the law enforcement community due to their non-binding nature (Interview, 2015h). For private industry, signing an MoU with Europol is good for their reputation as it can easily be used in the sales and promotion of products and services since the company can inform their customers that they collaborate with the law enforcement in the fight against cybercrime. It is, however, uncertain to what extent private industry can gain proof and what the legal consequences of their actions are.



[Figure 3.13.]: *EC3 Programme Board*

Source: Based on EC3 Programme Board website: https://www.europol.europa.eu/ec/ec3-board

The establishment of the EC3 advisory groups clearly demonstrate that the culture of law enforcement is changing in the field of cyber security and there is a need to reach out to non-law enforcement partners (financial services and academia), especially in the private industry. The reason this is significant is that the information that the law enforcement community requires to prosecute cybercriminals is often in the hands of private stakeholders. In other words, the law enforcement community has no other choice but to engage and establish partnerships with various law enforcement-friendly stakeholders in order to develop trust and a better exchange of information. Interviews with members of the AGs furthermore highlighted the significant role played by the private sector in providing technical support and expertise, since the private sector understand the cybercriminal structure. Therefore, it remains in the interest of EC3 to keep up positive engagement with financial institutions by convincing them that if they cooperate they will experience a much smaller loss from criminal activities of such nature.



[Figure 3.14.]: *EC3's Cooperation mechanisms*

Source: borrowed from Philipp Amann, EC3, Cybercrime challenges from LE perspective

However, one of the complaints coming from the private sector when collaborating with the law enforcement community is that the information flow is often one-sided (Interview, 2015i). This might be one reason why certain online social networking services, like Twitter, do not cooperate with the law enforcement community. Twitter states that in case of an law enforcement request for account information, users will be immediately notified about the request as 'Twitter's policy is to notify users of requests for their account information, which includes a copy of the request, prior to disclosure unless we are prohibited from doing so (e.g., an order under 18 U.S.C. § 2705(b))' (Twitter, 2015).

The other concern when it comes to information sharing is in connection with data protection. Some companies are more sensitive towards disclosing their customers' personal data for investigative purposes. The anxiety often raised by some private entities is that they are not authorised to provide customers' raw data, information sharing agreements or classified results as this would place the private company in breach of data regulations (Interview, 2015j). This raises the question of exactly what the communities (law enforcement, academia, private sector, and other government agencies) do understand under information sharing and what are the legal limitations. According to the new Directive of the EU Data Protection Reform, which was agreed by the EU Council and the Parliament in December 2015, the victim's data is fully protected (EU Commission, IP/15/6321, 2015). However, investigations often revolve around problems with the method of processing the attackers' data, since this can often not be investigated without touching upon the victims' data. Therefore, the question arises whether it would be feasible to form a public-private partnership (PPP) agreement on a method for information sharing about the attackers and criminals only, whilst making sure that the victims' data remains unharmed during a process which adheres to the data protection regulations.

4.1. J-CAT

J-CAT (Joint Cybercrime Action Task Force) was established in September 2014 in order to enhance the European response to cybercrime. J-CAT is regarded as the 'first physical, co-located and standing cybercrime task force' and is composed of cyber liaison officers from seven dedicated EU Member States (Austria, France, Germany, Italy, Spain, the Netherlands and the UK) as well as non-EU law enforcement partners

from Colombia, Australia and the U.S. (represented by three agencies the FBI, USSS and ICE) and EC3 which acts as the Secretariat of J-CAT (Reitano *et al*. 2015: 144). Most importantly, the cyber liaison officers are authorized only to report to and work for their corresponding Member States, hence, they are not dependent on Europol. The goal of creating J-CAT was to make it an EU taskforce rather than a Europol-led initiative (Reitano *et al*. 2015: 145). The reason for this is essentially a legal one, as having a Board and a leading Member State greatly enhances freedom and flexibility and overcomes all legal and bureaucratic hurdles, which allows J-CAT to respond to cyber threats quickly (Interview, 2015k). This flexibility of legal framework allows J-CAT to 'pragmatically follow the objective to proactively drive intelligence-led, coordinated action against key cybercrime threats and top targets' (Bergström *et al*., 2015: 473). Every single investigation is put forward to the J-CAT board as a proposal, and they then decide on cases they intend to pursue. Following the approval, a lead country is nominated to manage the investigation into the operational case (Reitano *et al*. 2015: 145). This legal flexibility also facilitates quicker collaboration between J-CAT and non-members. However, this pragmatic approach also raises responsibility concerns regarding the gathering and processing of data, legal remedies and liability issues of criminal justice policy (Bergström *et al*., 2015: 473). In addition, there are questions relating to what extent data is protected when it is shared between Europol and U.S. authorities (Bignami, 2007).

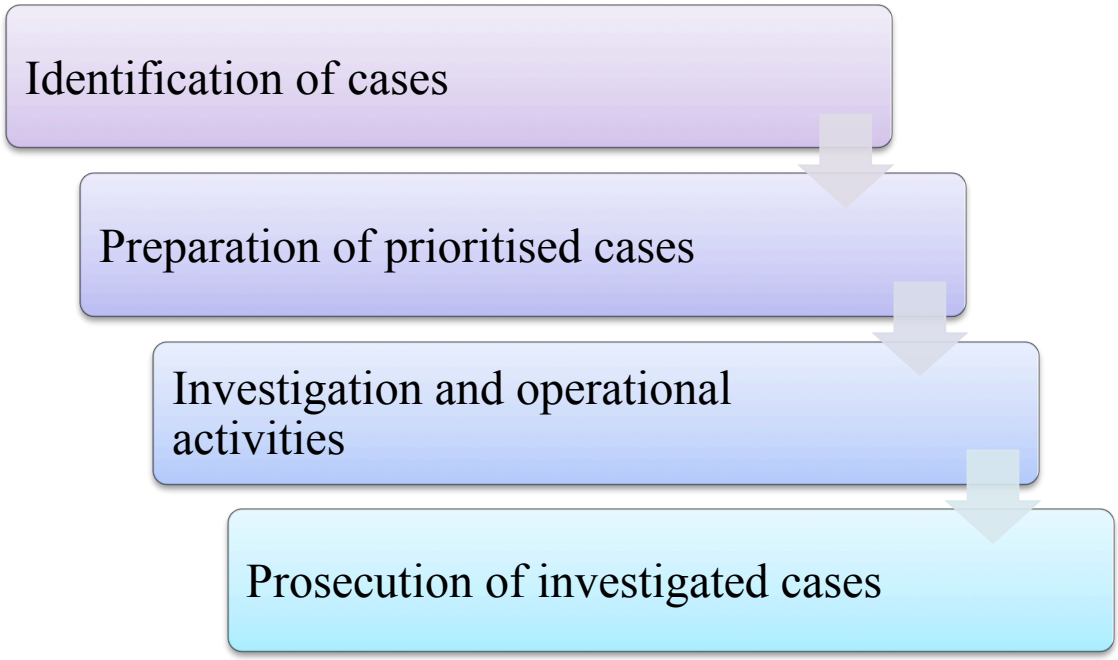
Furthermore, in order to start an investigation at J-CAT the approval of the Member State is needed. According to one of the J-CAT members, Europol's database is the best in the world (Interview, 2015k). In essence, J-CAT acts as a coordinating hub that helps accelerate exchange of information without having executive power. It also

has a stronger focus on arresting cybercriminals rather than advocating a preventive approach like the UK does (Interview, 2015k). J-CAT was born out of the frustrating, tiring and time-consuming traditional bilateral and multilateral collaborations that hindered efforts to counter the cybercriminal capacity to quickly form transnational deals and outpace the efforts of law enforcement (Reitano et al. 2015: 143). In other words, J-CAT replaced the very slow-paced, unsustainable interagency investigation process whereby investigators could take a few months to set up a meeting when shared interest were established.

Before J-CAT, the traditional form of cooperation could not be undertaken in real time as law enforcement agencies had to contact each other when information was requested or had to provide and then analyse data to discover any matches (Reitano et al. 2015: 143). Meetings were also often called where discussions among investigators took one or two days. In addition, it could take months before agencies checked whether any progress was being made (Reitano et al. 2015: 143). These challenges all highlighted the unsustainability of the system and the urgent need for change.

International cybercrime investigations covering a wide range of areas including attacks on children, targeting of high profile criminals and the stealing and selling of banking logins and personal data packages on the Dark Net have become more successful in terms of effectiveness and coordination since the launch of J-CAT (Bartlett, 2014). When J-CAT receives the approval of the Member State to start the investigation, it first collects all the relevant data regarding the specific cybercriminal case from the national entities, government and private partners (Europol, 2014a).

Once all the raw data is converted into 'actionable intelligence' then it will be put forward as investigative suggestions of possible targets and networks (Europol, 2014b).



[Figure 3.15.]: *Staged approach of the J-CAT*

Source: borrowed from Philipp Amann, EC3, Cybercrime challenges from LE perspective

In the first six months J-CAT carried out a number of successful operations such as the Ramnit botnet takedown in February 2015 that infected 3.2 million computers all around the world (Europol, 2015b). Criminals managed to gain access and control of the infected computers to deactivate their antivirus protection in order to steal banking and personal information. An interesting aspect of the botnet takedown under the 'umbrella of J-CAT' was that the operation was run in partnership with Microsoft, Symantec and AnubisNetworks, which demonstrated the potential for an LE-private partnership to work well for carrying out joint cybercrime investigations (Europol, 2015a). This might provide counterevidence for the assumption that the law

enforcement and intelligence community only gather information for their own purposes and there is a lack of two-way information sharing.

One J-CAT liaison officer noted that restricted membership has been one of the driving forces of the initiative in terms of strengthening trust amongst partners and sustaining vigorous intelligence exchange (Interview, 2015k). Furthermore, the success of the initiative is also manifested in the increasing number of effective international cybercrime investigations (for example, Operations Onymous, Imperium and Global Airport Action) (Europol, 2014b).

When it comes to intelligence sharing and trust building between the Member States and J-CAT, the agencies do not share intelligence directly with each other but rather with J-CAT. Member States are thus encouraged to provide knowledge to and develop trust in J-CAT, and to ensure that this trust is not broken; any available intelligence/information is given a handling code by the Member State who provides it (Interview, 2015k). This allows the Member State to determine how the intelligence can be used and to what level it can be shared.

Handling codes:
H0 – used as evidence in court
H1 – only for intelligence /police use – not for prosecutions
H2 – Restrictions: Very sensitive and state preserves its ownership. Only J-CAT has access to all H2 information, and other countries have no access permission. J-CAT can check the hits in the intelligence database and then accelerate bilateral or multilateral dialogues
H3 – Restrictions: intelligence is only shared between the 8 permanent Member States
There are **bilateral requests** in case there is ***a change of handling code***.

(Interview, 2015k)

This illustrates that handling intelligence under the right conditions can indeed develop trust and create a robust intelligence exchange. It might therefore be argued that the similar attitudes provide greater convergence in collaboration at the operational level, which is in contrast to the strategic-legal level where investigations are often delayed by the MLAT procedures. Convergence at the operational and law enforcement level might benefit from the development of an operational strategic cyber culture.

5. Conclusion

In conclusion, this chapter reflected on the theoretical work of Toje with the aim of examining how adaptive the concept of strategic culture is in the context of the EU cyber security policy. This chapter has therefore examined the three dimensions of EU strategic cyber culture: strategic, legal and operational. Firstly, it was suggested that as there is a lack of a single overarching EU strategic culture, the same assumption could presumably be applied when examining the EU approach to cyber security – specifically to cybercrime. Since the EU is not a single country, one has to take into account 28 different Member States that have their own historical baggage and mind-set regarding wider security issues and also the narrower matter of cyber threats. Clearly, the EU does not have a single cyber centre that deals with all aspects of cyber security, rather the tasks are given to different internal and external agencies or institutions, such as EC3, ENISA, CERT-EU and NATO, each with partial mandates. Therefore, it is suggested here that EU strategic cyber culture is fragmented and there are various cyber cultures that exist within the EU among the various mandates. Klimburg argues that there is seldom agreement between the three

dimensions of EU cyber policy, DG Home (cybercrime), the EEAS (common foreign and defence policy), and the DG for Economic Affairs (network and information security), and the EU treaties also provide each with different competencies (Klimburg, 2015). This often leads to much overlap and also confusion regarding who should speak on behalf of the EU on cyber security in the external realm (Interview, 2015e). For instance, whilst the EU–U.S. Cyber Dialogue is chaired by the EEAS, the EU–U.S. working group on cyber security and cyber crime is chaired by the EU Commission/DG Home. Furthermore, since cybercrime is borderless by nature, it is widely acknowledged that dealing with the problem of multiple jurisdictions is making investigations ever more difficult for law enforcement authorities.

The chapter also examined both the drivers of and obstacles to EU SC and looked at the way EU SC has been formed under CSDP and how the EU perceives and responds to security threats. The discussion then examined the non-static nature of the development of strategic cyber culture at the EU collaborative level and it suggested a linkage between CSDP and cyber defence as a starting point for this "evolution". Moreover, the discussion continued to broaden the concept of EU strategic cyber culture by "looking out of the defence box" and analysing the strategic and legal dimensions of EU cyber culture in an expanded frame. This provides a better understanding of the decentralised and fragmented approaches that exist on the EU level which nevertheless boast their own distinct identity and now increasingly effective operations.

Chapter IV.

U.S. strategic cyber culture

"There's no way that we are going to win the cyber security effort on defense. We have to go on offense."
Steven Chabinsky
(Former head of the FBI's cyber intelligence section)

The word 'cyberspace' was first coined by William Gibson in 1982 as part of the short story, 'Burning Chrome'. It was Gibson's 1984 debut novel, *Neuromancer* that further theorised the virtual network. Gibson has explained that the inspiration behind it came from watching children playing arcade games: 'It seemed to me that what they wanted was to be inside the games, within the notional space of the machine … and somehow I knew that the notional space behind all of the computer screens would be one single universe' (Jones, 2011). However, what differentiates the cyberspace Gibson envisioned in *Neuromancer* from today's modern Internet is its largely textless nature.

The modern Internet has brought both positive (benefits) and negative (risks) consequences. This dichotomy lies in its openness, which provides incomparable strategic innovation and collaboration, but also a myriad of tactical "victories" for attackers. Online crime infiltrates almost all layers of society, including the private sector and government, and has an impact on all Internet users. Therefore, cybercrime is considered as one of the most pressing issues and fastest growing forms of crime that the U.S. - along with the EU and other countries - faces today. The PWC Global Economic Crime Survey 2016 reports that cybercrime has gone from being the 4th-most reported economic crime to the 2nd- most reported economic crime over recent

years (PWC, 2016a). The Internet is widely considered the 'cheapest' and most effective option for criminals due to the ubiquitous anonymity that networked access provides, and the ease with which the Internet can be taken advantage of. Furthermore, criminals only have to figure out how to utilise limited computer expertise in order to make a profit through attacks launched in cyberspace. According to Steven R. Chabinsky, cyber criminals 'have evolved their practices to make their crimes more profitable ... They choose specialties, master their skills, create networks of colleagues, and organize their crimes' (Chabinsky, 2010). Moreover, we also need to remind ourselves that cyber criminals are fast learners who display good adaptability skills, especially within the prison environment, which provides sufficient learning tools to allow perpetrators to acquire anti-surveillance computer skills (OIG, 2014).

Nevertheless, despite the intermediate nature of current cybercrime, most policy makers and legal experts agree that the U.S. remains unprepared to tackle the rising wave of cybercrime that poses a threat to the country's national security, including the protection of critical infrastructures, freedom of expression online and the economic sustainability of U.S. businesses (Bucci et al., 2013).

The belief that even a government as large as the United States' government is incapable of fighting cybercrime alone is one that appears to represent the consensus at recent cyber security conferences. Consequently, the U.S. government has been reaching out to international partners that share similar values, such as the EU. In order to understand what drives the States' behaviour when collaborating with international partners (e.g. the UK, Australia, Canada, Israel, etc.) in the fight against

cybercrime, it is necessary to understand the strategic cyber culture that underpins U.S. policy.

It is logical to argue that even if cybercrime cannot be completely eradicated, its effective containment depends on multi-layered collaboration and responses due to its own multi-layered nature. Accordingly, most state responses are likely to be both dispersed and complex. Therefore, this chapter will advance the proposition that the U.S. is too large to command a single strategic cyber culture and will examine why U.S. strategic cyber culture is fragmented rather than unified.

[Figure 4.1.]: *U.S. fragmented strategic cyber culture*

As illustrated in the above figure, the numerous stakeholders – each of whom forward their own perspectives on cyber security and solutions – partially explain the fragmentation of U.S. strategic cyber culture. In essence, whether it comes from law enforcement, the intelligence community, industry or academia, each approach within U.S. strategic cyber culture will bring fragmentation to the system and potentially cause conflicting interests. Therefore, it is suggested that fragmentation is not essentially an inevitable aspect of cyber security (Van der Meulen et al., 2015: 103).

Given the above analysis, the argument that there is more than a single all-encompassing strategic cyber culture in the U.S. is proposed in this chapter. Given that there is more than one cyber culture present within the U.S. at the federal level, this generates different approaches, leads to fragmentation, and makes the U.S. response to cybercrime somewhat more fragile. Therefore, this section of the thesis will focus on challenging scholars such as Cavelty and Healey, who assert that the U.S. approach is merely dominated by an attempt at militarising cyberspace. In this chapter, it is instead suggested that militarisation is only *one* facet of U.S. strategic cyber culture. The concept of strategic culture must be extended to three separate levels in order to rethink the approach taken to cybercrime in the U.S. and better understand the fragmentation of divergent approaches present in the country. These three levels are strategy/policy, legal services and operational dimensions (including military and law enforcement).

At the *policy* level, strategic cyber culture reflects the government's approach to the development of policies (both public-public "PuP" and public-private partnerships "PPP") and diplomatic relations (the use of soft power) in the fight against cybercrime.

At the *legal* service level, strategic cyber culture represents the organisational culture – values, missions and technologies – that an institution (e.g. the Department of Justice) or legal authority adheres to closely and that affects the way criminal laws are advanced in order to tackle cybercrime.

At the *operational* level, strategic cyber culture is an expression of how a nation's military and law enforcement agencies tactically address cybercrime; or, in other words, apply the use of force in practice. It is possible to determine the driving forces behind the United States' collaboration with the EU through the exploration of the U.S. approach to strategic cyber culture in relation to the fight against cybercrime at different levels. This exploration also allows for the influence of strategic culture to be mapped effectively in various contexts.

Again, this chapter argues that the U.S. government - in parallel with the EU's governing elite – should not be considered a 'monolithic' entity in its approach to cyber security, especially in the case of cybercrime. Similarly, this aspect of the current thesis is focused on identifying the main carriers and driving forces associated with U.S. strategic cyber culture. Thus, this thesis questions the role of large U.S. companies, agencies, the government, and White House cyber czars and commissions. To illustrate the differences in approaches, it can be said that on the one hand, diplomats from the State Department aim to promote an "attractive" of the U.S. as being committed to an open, free and secure Internet with peaceful terms – a "soft power tool" that holds the potential to influence others and achieve goals through persuasion, diplomacy, propaganda or economic aid. On the other hand, at Fort

Meade, cyber warriors (U.S. Cyber Command) and the intelligence community (NSA) are working towards full spectrum dominance with larger budgets and authority (Healey, 2013). The approaches taken to cybercrime by U.S. federal agencies (i.e. the FBI, DHS, DoD and Immigration Customs Enforcement (ICE)) are similarly contradictory, although more complex.

This chapter begins with the proposal of four key assumptions as to why fragmentation is deeply embedded in the operational, legal and strategic levels of U.S. cyber culture. This chapter will then present a brief overview of the key characteristics associated with U.S. strategic culture. These characteristics are presented with a traditional view that examines the relationship between U.S. strategic culture and cyber power, with recognition of the influence of history and corporate memory as a tool for mapping changes in regulatory, military and cyber policy. This will serve as an explanation as to why war culture is so entrenched in U.S. culture and why the militarisation of cyberspace plays such a major role in U.S. strategic cyber culture.

The suggestion that the relationship between counterterrorism and cyber offense could represent the starting point in the development of a fragmented U.S. strategic cyber culture is then presented. The following sections then place greater emphasis on the non-militaristic aspects of U.S. strategic cyber culture at the strategic, legal and operational level by focusing on the fight against cybercrime.

In the second part of this chapter, policy dimensions will be explored in terms of the promotion of U.S. cyberspace norms. This chapter will then touch upon the way in

which cyber security policy issues have been developed under each of the U.S. Presidents, beginning with Reagan and ending with Obama. A brief overview of the vital cyber policy issues that have been developed under each President will then be presented from the perspective of strategic culture. The main focus of this section will be on the cyber policy issues developed under President Obama who – according to Stanford President John Hennessy – is considered 'the first president to truly understand cyber security risk, because he is the first president to be constantly digitally connected' (Stanford Report, 2015).

The third section of this chapter demonstrates another non-militaristic approach taken to the fight against cybercrime at the legal service level within U.S. strategic cyber culture. Finally, the chapter ends with a focus on the operational level and the methods adopted by federal agencies to combat cybercrime.

Before proceeding, one important point should be reflected upon. Whilst the EU consists of 28 different Member States – each carrying its own distinctive historical baggage - the United States consists of 50 states, 5 territories and 1 federal district (Washington, D.C.), each of which is governed on both a federal and state level. Whilst the 50 U.S. states' freedom from language and cultural barriers might suggest easier governance than, say, the EU's governance of Brussels, cyber threats move at different speeds depending on the specific state, as do the regulatory and legislative processes associated with them.

Exemplifying this, it is commonly noted that there are differences between the activities of the East and the West Coast, divided between the "West Coast coders"

(i.e. software) and the "East Coast coders" (i.e. policy and law makers) (Interview, 2015l). Nevertheless, since policy, regulation and legislation represent a key part of this research - and because there are certain limitations to the available time and resources - the East Coast coders alone will serve as a valuable point focus in this chapter.

1. Fragmented U.S. strategic cyber culture

First and foremost, it is important to note that there is remarkably little discussion about the huge competition manifesting itself at the federal level amongst various agencies, and even less about the way that this prompts disjointed responses when dealing with cases of cybercrime. The United States' issues in collaborating with international partners stem from the lack of a unified voice amongst those various government layers and agencies that play a major role in the government's response to cybercrime in partnership with the private sector. Although the characterisation of the U.S. "militarising" cyberspace by many scholars may be accurate with respect to U.S. Cyber Command, it is not necessarily reflective of, or anywhere close, to the overarching direction of U.S. cyber security policy. Indeed, it may be that the alignment of U.S.-EU policies originates from the decidedly less militaristic view that agencies such as the State Department or DHS take towards cyberspace; a view that places them more greatly in strategic alignment than dis-alignment with the EU.

As demonstrated in Figure 4.1, the fragmentation of the U.S. cyber ecosystem is driven greatly by public and private sector stakeholders' pursuit of self-interests, as well as the diversity in definition of cyber threats themselves. This can be seen in the

case of federal agencies as much as it can in any other stakeholder (see below Figure 4.2)

[Figure 4.2.]: *U.S. federal approach to cyber security - responsibilities*

Another important reason for the struggle between U.S. federal agencies is the congressional indecision on cyber security legislation and the hesitancy over which agency should take the lead in tackling cybercrime (Interview, 2015m). A recent study entitled *Influencing the Bureaucracy: The Irony of Congressional Oversight* was conducted by Vanderbilt researchers who surveyed 2,400 federal executives in order to assess the extent to which federal agencies are politicised and to whom these agencies are more responsive: the White House, the congressional oversight committees or the majority party of the Congress (Clinton et al., 2014: 2). Interestingly, the findings indicated that the US Congress has less of an influence than the White House:

> We find that when more committees are involved in monitoring and potentially directing agency policymaking, Congress is less influential than the president for determining agency policy. Increasing the number of involved committees may maximize the electoral benefits for members and provide a platform for making public proclamations on issues of importance, but it appears that an increase in the number of committees also undercuts the ability of Congress to respond collectively to the actions of the presidency or the bureaucracy.
> (Clinton et al., 2014: 3)

These findings also strongly suggest that federal agencies are politicised at the top level because of the influence coming from the White House, as represented by political appointees. This may explain the lack of community between federal agencies, replaced with vigorous competition, as well as the politicisation of responses to cyber threats.

The politicisation of cyber threats at an early stage could be regarded as another distinctive characteristic of U.S. strategic culture when countering cybercrime.

Cavelty argues that the existence of strong politicisation could be linked to the "overrated" rhetoric, provided by bureaucratic entities regarding threats, arguing that serious action is needed due to the grave threat that a large-scale cyber attack poses to national security (Cavelty, 2012: 115). This rhetoric behaviour and "urgency" amongst the various agencies and entities could also be explained by the competition over political influence and budgetary resources (Cavelty, 2012: 116).

This analysis was supported during an interview with a former NSA and DHS employee, who argued that political appointees dominate the highest levels of the federal civil service system (Interview, 2015n). This explains why there is so little long-term investment in consensus building. In an interview with a HM Government principal technical specialist, the same perspective was shared through the following statements:

> In the U.S. political appointees go quite deep into the hierarchy and rather than being concerned with strategic guidance of the organisation they also make decisions on the tactical and operational levels.
>
> This stands in notable contrast with the EU where decisions both at the tactical and operational levels are decided by government employees and not by political appointees – in other words, it is less politicised and actors have a long-term investment in building a community.
> (Interview, 2015l)

Inter-agency relationships now feature significant distrust as a result of their overt politicisation at the leadership level. This culture of mistrust, common between U.S. federal agencies such as the FBI, DoD, ICE, DHS and DoJ, could explain why it has taken a couple of years for them to collaborate with on another more effectively on matters related to cyber security. This is accelerated by the sizeable budgets that the

U.S. has allocated to this area, allowing some scope for duplication and rivalry (see Table 4.1).

[Table 4.1]: *FY 2016 Agency Spending*

Department or Agency	Outlays
Dept. of Agriculture	$137,740,057,327
Dept. of Commerce	$9,429,415,979
Dept. of Defence - Military Programs	**$516,237,907,560**
Dept. of Education	$70,850,949,480
Dept. of Energy	$24,557,506,270
Dept. of Health and Human Services	$994,650,662,844
Dept. of Homeland Security	**$46,371,372,268**
Dept. of Housing and Urban Development	$25,699,570,046
Dept. of the Interior	$12,560,014,331
Dept. of Justice	**$35,036,725,188**
Dept. of Labour	$39,005,732,712
Dept. of State	**$27,688,104,621**

Source: Borrowed from 2016 United States Budget Estimate, FY 2016 Agency Spending. Available at http://federal-budget.insidegov.com/l/119/2016-Estimate

At a more fundamental level, we might argue that the U.S. federal government has always been fissiparous and indeed was designed to be so. The lack of harmony and 'battle against the political domination over the selection of public employees' dates back to the Jackson presidency (1828-36) (Peters, 2004: 125). The U.S. has been described as embodying a 'spoils system' that was well institutionalised at that time, with politicians dictating the majority of federal government positions (Peters, 2004; Chaudry, 2012; White, 1965). The 'spoils system' was strong in the beginning and still continues today. It is for this very reason that political appointees "loyal" to the incoming president's policy replace the entire upper level of the government in the event of a new administration after a four-year term (Chaudry, 2012).

Whilst a number of initiatives, such as the Pendleton Act (1883) and Hatch Act (1939), were introduced in order to create more transparency, the top level of the public organisation pyramid remains both opaque and overly politicised (Peters, 2004). The 'historical legacy of the spoils system' that remains a feature of the U.S. today offers a macro-level explanation as to why the issue of cyber threats has become highly fragmented at the political leadership level of the federal agencies. This interpretation is strengthened by similar behaviour within the U.S. government in other areas of increased security spending, such as intelligence or the Special Forces.

The absence of specific law or regulation defining cybercrime serves as another contributing force to the disjointed U.S. response to cyber threats. According to the United States Code (USC) cybercrime is treated as a method, not a category such as bank robbery or kidnapping (Santanam, 2010: 41). Santanam also adds that cybercrime is not a recognised legal term, with lawyers instead tending to refer only to "computer related offenses" (Santanam, 2010: 41). This ambiguity in terminology, together with the inaction in officially defining cybercrime, is also highlighted by the recent CRS report, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement* (Finklea, 2015). Since there is no official U.S. government definition of cybercrime, federal law enforcement agencies are often left to define it *en passant* within their own jurisdictions and investigations (Finklea, 2015). No single agency has been allocated to as a lead investigative agency in order to combat cybercrime, which is in part due to the lack of clarity in the definition of the term (Finklea, 2015; Interview, 2015m).

Finally, the deeply-rooted perception of the centralised federal government as "evil" provides another reason for the fragmented response to cyber threats in the U.S. This could be regarded as a distinctive characteristic of U.S. strategic culture and is in sharp contrast with European mentality. It is partly for this reason that the U.S. has no single national police force, since the American public is highly conscious about surveillance and the abuse of police power (Interview, 2015o).

This point can be illustrated through a point raised in relation to Canada during an interview with a U.S. FDA officer:

> Despite the fact that in Canada the single national and federal police force (the Royal Canadian Mounted Police (RCMP)) runs successfully – well established within the Canadian strategic culture and does not create public fear that police power might be abused - it would be impossible to introduce this in the U.S. More than that, if for instance there would be no CIA and today - if it was proposed to create a CIA it would most likely fail due to the lack of public support.
>
> (Interview, 2015p)

Meanwhile, if several U.S. federal agencies were dealing with security threats such as cybercrime, with each applying their own methods and approaches, it gives the public the impression that government power is "equally" balanced and checked. In other words, it is considered better to retain the lavish budgets that generate "turf battles" and competition amongst the federal agencies than to create a single police force that would trigger even greater distrust towards the government. Since partnerships with overseas agencies tend to offer mutual benefits and a lack of competition, these partnerships tend to be more effective than those between U.S. federal agencies (Interview, 2015n).

1.1. *Understanding the American "psyche" and mindset on the use of force*

The critical issue here is that strategic culture is historically constructed. Russell Weigley's well-known study, *The American Way of War,* argues that there is a specific and well-developed strategic culture in the U.S., especially when it comes to the application of 'hard power' - coercive means such as military force (Weigley, 1977; Klare, 2015). In his landmark survey, Weigley provides an in-depth analysis of the U.S. strategic approach based on data form the past 200 years, arguing that American strategic culture has – in Clausewitzian terms – been dominated by the spirit of the 'absolute' form of war from the George Washington era to the time of Robert McNamara (Harris, 2008: 75; Weigley, 1977). Weigley particularly argues that its intellectual roots lie in Jomini's work, *Art of War,* which exercised a major influence on American military thinking and war culture (Weigley, 1977). American war colleges, first developed during the 19th century, followed the writings of Jomini very closely. This work featured a significant number of maxims, rules and principles that rationalised war and made it comprehensible. In other words, the U.S. has long featured a hypo-rationalisation of the analysis of strategic culture and war culture. This could be thought of as one important strain that historically feeds into what was to become the Pentagon culture (Faber, 2012).

In contrast, some argue there is little evidence as to whether Jomini's work on principles and rules was read extensively by the American officers before the Civil War. Therefore, Hope suggests that since very few could read in French, the majority of the U.S. public was not familiar with Jomini's writings during the Jacksonian era (Hope, 2015).

According to Peter Faber, U.S. strategic culture started to embrace American Progressivism with business variations ('Taylorism') at the turn of the 20th century (Faber, 2012). Theodore Roosevelt and other progressives were fascinated by the scientific efficiency emerging in American factories, such as the precision introduced by Frederick Taylor and others in production lines. Taylor considered bureaucracy 'a solution to ideological cleavages, as an engineering remedy to the war between the classes' (Carson, 2011; Shenhav, 2002: 8). It was concluded that the principles behind such enlightened business practices could be applied to the federal government. Therefore, Roosevelt and his fellow reformers anticipated a golden opportunity to address the waste created by the "dusty" bureaucratic system that had been in place in the 19th century War Department. Essentially, it is suggested that the 20th century began with a Jominian-inspired strategic culture before moving on to embrace the efficiency-oriented progressivist business practices of later years (Carson, 2010).

Rising American enthusiasm for technology as a force multiplier in the application of hard power became the third important factor in the establishment of U.S. strategic culture later in the 20th century. This, together with the ideas discussed above, ultimately created the major features of U.S. strategic culture today and provided a foundation for the American way of war. On the other hand, Colin Gray describes American strategic culture as follows:

> … modes of thought and action with respect to force, derived from perception of the national historical experience, aspiration for self-characterization ... and from all of the many distinctively American experiences (of geography, political philosophy, of civic culture, and "way of life") that characterize an American citizen.
>
> (Gray, 1981: 22)

This, therefore, prompts the question: What are the major characteristics and drivers of U.S. strategic culture?

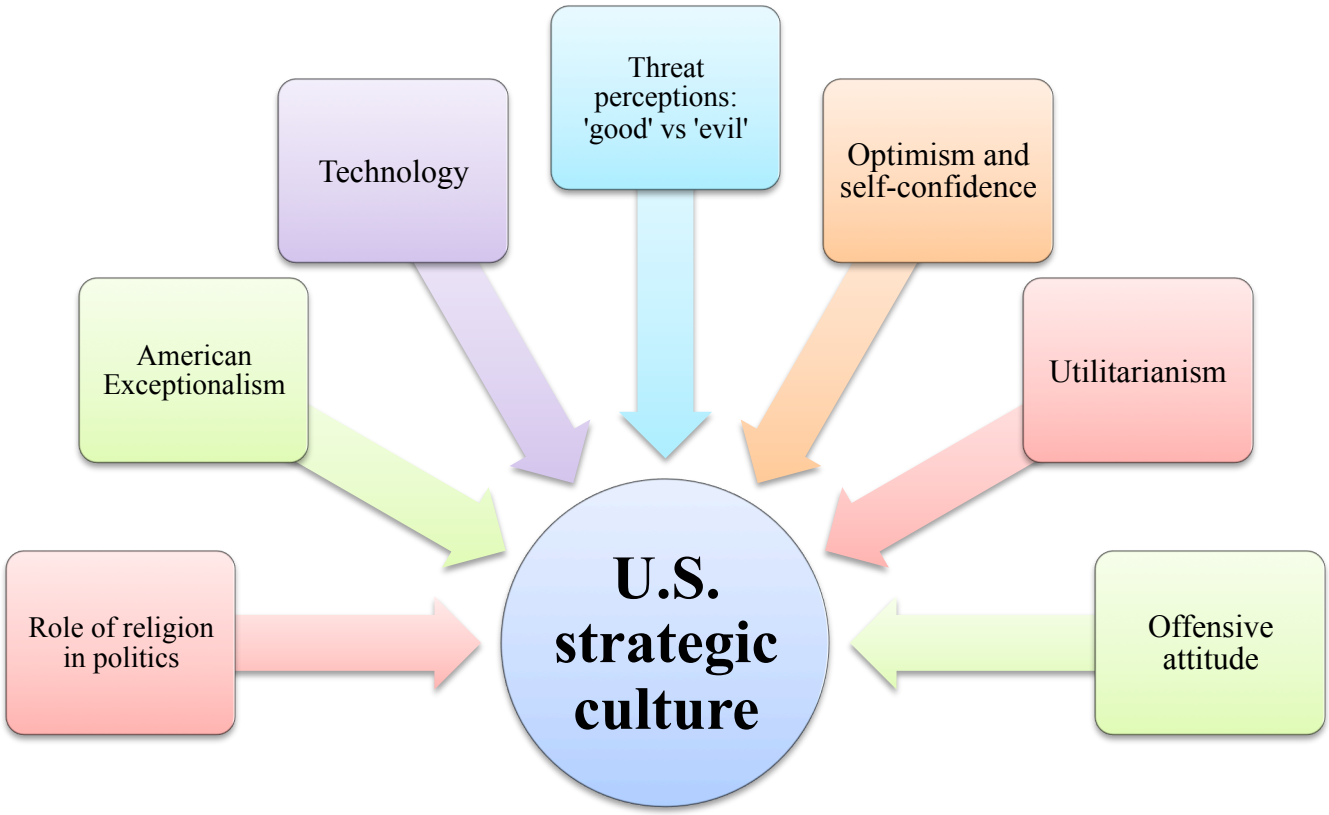
The field research conducted in Washington DC during the summer of 2015 confirmed some of the major assertions suggested by scholars (e.g. Hampton, Gray, Faber, and so on) about U.S. strategic culture (see Figure 4.3, below). The following section therefore explores the ways in which U.S. strategic cyber culture features, and is influenced by, these characteristics.

1.2. Drivers of U.S. strategic culture

There is considerable debate about the long-term cultural factors that influence U.S. behaviour and decision-making. Not only is the U.S. considered the world's primary 'superpower', it is also the EU's most important strategic ally. Approaching this notion through the lens of U.S. strategic culture helps to reveal the ideological difference between the U.S. and the EU in terms of security threats (e.g. law enforcement and judicial cooperation) (Marsh & Rees, 2012: 59). The differences between the U.S. and EU are also reflected in their divergent strategic and legal responses to cyber threats.

A number of perspectives regarding U.S. strategic culture and the American way of war were highlighted in the interviews conducted in Washington DC. These are summarised in Figure 4.3. First and foremost, it is suggested that the American way of war is practical and utilitarian, and that the Department of Defence is particularly solution-oriented. Secondly, it is proposed that American culture is optimistic, representative of a "can do" attitude, where one seldom hears anybody (for instance,

in the Pentagon) immediately saying "no, it cannot be done". Thirdly, the interviews suggest that the U.S. has an affection towards, and dependence on, technology as a problem-solving tool in the diplomatic arena. Fourthly, U.S. strategic culture is seen as firepower-oriented, and it often emphasises historical "masses" (e.g. its large standing professional army) by bringing together large numbers of technologies against an opponent. The U.S. is also perceived as offense-focused and aggressive, rejecting of the idea that the collision of strategic cultures can be achieved through defence. Finally, the U.S. is considered as being characterised by a short-term, somewhat impatient orientation (Interview, 2015n).



[Figure 4.3.]: *Drivers of U.S. strategic culture*

Source: Based on interviews in Washington, D.C. (2015) and from Hamilton (2013)

American exceptionalism

The U.S. has been often been stereotyped, by both American and European academics, as displaying 'American exceptionalism'[10] as a result of having great military power and being one of the richest countries in the world. This has led many policy-makers in Washington to assume American superiority is natural in all contexts (Kohut & Stokes, 2006). However, some argue that this makes America akin to the 'exceptionalism' of Greece or Britain (Walt, 2011).

Exceptionalism can be traced to the 1774 Articles of Association – 'one of the early acts of the First Continental Congress' (Litke, 2013: 92). Americans regard themselves as God's chosen nation: members of a Promised Land that adheres to its core values of liberty, freedom and the American way of life that they so much want to protect and, indeed, export. Thus, America's tendency to be "called on to counter evildoers" makes logical sense, given the country's self-assessment as a force of overall good (Hampton, 2013: 30).

Those who disagree with such labelling argue that the U.S. only pursues its own self-interest and, like any other great power in the past, has convinced itself that it is a different and better nation than the rest (Walt, 2011; Interview, 2015q).

Role of religion in politics

[10] American exceptionalism refers to the notion that the U.S. and the American people hold a special place in the world, including its values, history and political system, that is worthy of universal admiration. It also suggests that the U.S. is both predestined and authorised to fulfil a distinctive and positive role in the world.

Since America is one of the most religious nations in the industrialised world, it is assumed that this religiosity plays an important role in determining public and elite perceptions of foreign policy and threats (Hampton, 2013: 25). George Washington noted, 'Do not let anyone claim to be a true American . . . if they ever attempt to remove religion from politics' and also demonstrated the strong connectivity between morality, American national identity and religious conviction (Kohut & Stokes, 2006: 100). The idea that 'Americans think that being religious is a prerequisite for being a 'good American'' is supported in Robert Putnam's recent work, *American Grace* (Putnam & Campbell, 2010: 541; Hampton, 2013).

Religious views - and more importantly, religious language - have clearly played a formative role in elite perceptions of the nature of threat and have therefore contributed to the approaches and policies of most administrations (Hampton, 2013: 33). President Woodrow Wilson and John Foster Dulles, secretary of state under President Eisenhower, all arrived at this intellectual point of focus as a moral imperative for foreign policy. This point can be illustrated through the work of Wilson, who spoke of the role of good and evil in world politics:

> The field of battle is the world. From the abodes of righteousness advances the host of God's people under the leadership of Christ . . . From the opposite side of the field, advancing from the tents of wickedness, come the hosts of sin led by the Prince of Lies himself, riding upon death's horse.
>
> (Wilson, 2005: 71-72)

With numerous modern-day presidents, including Reagan, Carter and Bush, having similarly emphasised that religious awakening transformed their views of the world, Wilson is not alone in his ideology. President Barack Obama has also confirmed his

Christian convictions and their impact of foreign policy (Pulliam & Olsen, 2008). Rotter maintains the following point:

> Even in an ostensibly secular state the private religious commitments and concerns of foreign policy-makers can be crucial, even decisive, factors in shaping international relations, especially when the policy-makers share a common religious culture.
>
> (Rotter, 2002: 593-613)

Rotter, and indeed many other seasoned observers, argue that these ideas strongly influence the overall texture of U.S. foreign and security policy (Rotter, 2002: 593-613; Kirby, 2003: 4; Hampton, 2013: 33). These actors assert that a 'Protestant missionary subculture' emerged in Washington DC over time as a result of devout political elite dominating the U.S. foreign and security policy establishment (Hampton, 2013). Accordingly, in his book, *Woodrow Wilson: A Biography,* John Milton Cooper quotes President Wilson, explaining that the foundation of America was 'for the benefit of mankind as well as for the benefit of its people'. This point continues to be the cornerstone of American strategic culture today (Cooper, 2009: 583). Consequently, the common assumption of an ideational and moralistic U.S. foreign policy dates back to the very founding of America. Recent figures show that whilst a decreasing number of Christians reside in the U.S. today (based on data from 2007 to 2014), America is still home to 'more Christians than any other country in the world' (Pew Research Center, 2015).

Threat perceptions: good vs. evil

According to Kohut and Stokes, the majority of Americans 'see their religious beliefs as the basis for America's success in the world'. Accordingly, intellectuals and elite leaders tend to identify the nature of a threat in terms of 'good' and 'evil', often

deploying idealistic or even messianic language when offering public justifications of policy (Kohut & Stokes, 2006: 97). The conviction that the U.S. can only be survive threats with the help of 'providential guidance and the mighty force' underpins this perspective (Hampton, 2013: 30).

For instance, the immediate reaction of the U.S. to the events of 9/11 was to condemn terrorism using religious language, talking of 'evil' and the 'bad guys'. This can be seen clearly in the speech given by former President George W. Bush following the attacks:

> We have been warned that there are evil people in this world […] As I said yesterday, people have declared war on America, and they have made a terrible mistake because this is a fabulous country […] My administration has a job to do and we're going to do it. We will rid the world of the evildoers.
> (Bush, 2001a)

Both McDougall and Hartz argue that Americans have perceived external threats as "evil" since the 17th century, and that this demonisation of foreign dangers still exists today (Hartz, 1991; McDougall, 2005: 109). It could be argued that the speeches of Bush following 9/11 can be linked to the original philosophy of the Pilgrim Fathers in their claim that government actors are chosen by God, thus representing 'goodness'.

In 1620, the Pilgrim Fathers (English Puritans and Separatists) escaped from England on a ship called the Mayflower, sailing from Plymouth to North America in pursuit of religious freedom. In order to avoid religious persecution from the Church of England and to be able to practice their religion freely, they fled to New England and founded the 'Plymouth Colony' (known today as Plymouth, Massachusetts). The social and legal systems of Puritan New England already represented the strong relationship between religion and politics at the time. Government leaders were also church

members, considered to be God's chosen people (Edel, 1987). Colonists who wanted to become full members of the church had to endure numerous tests to prove their faith was strong. Therefore, it is suggested that the customs developed in the Plymouth colony have been a determining factor not only in the development of the American political and legal system we see today, but also in the country's cultural-religious beliefs.

Furthermore, there is a wide consensus within academic circles studying U.S. culture and history that the nature of external threats constitutes an essential ideological component what Americans have always been fighting for: preservation of the American way of life, liberty and the belief that they belong to a nation chosen by God, and therefore assigned the duty to fight evil and – if necessary – bring 'light' to the world (Hampton, 2013: 32). Based on this notion, it would be considered the responsibility of the U.S. government to protect the American population from 'evil': or, in other words, from terrorists, radical extremists, Islamists and 'evildoers'.

However, like the EU, U.S. strategic culture has its own weaknesses. For instance, scholars such as Faber (2012) argue that it is America's lack of cultural awareness and historical context, as well as its heavy idealism, that cause the country's strategic culture to be problematic. Whilst the U.S. military has historically revered Clausewitz, the Pentagon's strategic culture and American way of war do not demonstrate strong Clausewitzian connections but, instead, flexible and weak connections to political objectives (Faber, 2012). Hassan characterises the American way of war as an anachronistic 18th century approach, arguing that this cognitive outlook causes damage to the Army in its attempts to be innovative and adapt to the

current era of persistent conflicts (Hassan, 2015: 90). Therefore, this misleadingly reaffirms the assumption that the nation has the capacity to raise a large professional army of fresh recruits at very short notice (Hassan, 2015).

This raises the question as to how this approach to the use of force affects U.S. strategic cyber culture and whether it could provide an explanation as to the dominating militaristic aspect of U.S. strategic cyber culture.

The non-static nature of the evolution of U.S. strategic cyber culture can be better understood with a brief introduction to its nature and main features, such as the approach taken to war, the use of force, and the perception of threats. As noted throughout this chapter, U.S. strategic cyber culture is fragmented rather than one single militaristic culture. Here, both state and sub-state actors bring their own experiences and mentalities to the table when dealing with cybercrime. Nonetheless, the militaristic behaviour of the Department of Defence, USCYBERCOM and Fort Meade plays a vital role and represents the starting point of the construction of U.S. strategic cyber culture.

One of the central questions to be asked when analysing U.S. strategic culture in relation to cybercrime is which institutions and organisations act as keepers and sources of U.S. strategic cyber culture: the U.S. Department of State, the military, or perhaps only a subset of the military or the intelligence agencies? Another challenge lies in investigating the content of strategic cyber culture - the beliefs, attitudes, values that it embraces – as well as to what extent strategic culture determines the approaches and behaviour demonstrated by the U.S. (Booth et al., 1999: 8-12;

Mahnken, 2006: 5). Healey argues that many lessons from U.S. cyber conflict history are often ignored despite there being a reasonable amount of relevant experience to learn from (Healey, 2013: 16). Therefore, it appears as if each generation learns from its own experiences, not from the mistakes of previous generations. The idea that we must experience something first-hand if we are to truly learn from it is noted as a common human behaviour by sociologist researchers working in the field of learning theory.

Furthermore, it should be noted that the interviews conducted in Washington D.C. as part of this dissertation suggest that there is often tension between law enforcement, military, legal authorities, the government and society as a whole, at all levels.

1.3. Evolution of U.S. strategic cyber culture

The dynamic evolution of federal-level U.S. strategic cyber culture will be explained over the following sections. In this thesis, it is suggested that the starting point in the development of U.S. strategic cyber culture may be the identification of the link between cyber offences and counterterrorism. The reasoning behind this proposition is related to the widely held assumption that the American response to security threats is rooted in terrorism and organised crime, which prompts similar responses to cyber threats. That is, responses are driven by the fear of threat to national security, which only the military can counter. This chapter attempts to challenge this assumption.

From the perspective of strategic culture, it is often suggested that the U.S. has pursued a narrowly militarised offensive cyber security policy that, on an operational level, perceives the Internet as the fifth domain of warfare. Additionally, the

development of an offensive U.S. cyber command suggests that the Internet is considered a battleground rather than a collective commons that facilitates mutually beneficial human development. Whilst it can be seen that this argument has some truth to it, this is only part of the story. Since both the military and cyber offence play an important role in the U.S. approach to counter cyber threats, the following sections will be demonstrating the U.S. militaristic mind-set that constitutes a major part of U.S. strategic cyber culture.

The military language of American cyber security is convoluted. There is the assumption that the main driver of the U.S. approach to cyber security is to defend against a possible cyber 9/11; or, in other words, a 'Cyber-Pearl Harbor'. This is due to the fear of an unexpected massive cyber-attack on the nation's grid that could be triggered by foreign nations. However, the consideration of, and reference to, cyberspace as a battleground suggests that the U.S. advocates operational offense. Despite this, no specific details on the application of such offensive competencies are provided in the cyber strategy launched by the DoD in 2011. In comparison, the DoD strategy released in April 2015 – considered to be a more comprehensive overview than the 2011 strategy – aims to be more transparent about U.S. doctrines concerning military roles and missions in cyberspace. Thus, this provides a clearer picture of the DoD's role in defending the nation against cyber attacks as well as how cyber capabilities will be integrated into military operations (DoD, 2015). The application of deterrence suggests that cyberspace is viewed as an operational domain of warfare, which has been acknowledged as a new domain within U.S. military doctrine (Cavelty, 2012: 119). Furthermore, in the White House's *International Strategy for Cyberspace*, it is explicitly argued that the U.S. has the right to project military force

in order to counter hostile attacks in cyberspace (Obama, 2011). Thus, it is clearly demonstrated that in order to project deterrence, the U.S. keeps the potential of an asymmetric response an open possibility.

Therefore, in order to maintain the 'active' defence position – driven by the fear that national security is under threat - the U.S. advocates increasing its cyber power through military means (Nye, 2011). The information presented in the Snowden leaks confirms that the MonsterMind programme has been developed not only for the purpose of detecting cyber strikes against U.S. servers, but also to permit automatic fire-back against an alleged attacker without authorisation (Zetter, 2014). The risk that this may cause escalation and catalyse a cyber war has been raised as a concern.

1.4. The rise of the military Internet complex

Originally, the Internet was part of a U.S. Department of Defence (DoD) project called ARPANET, which started in the 1960s with the objective of building a nationwide computer network system (Cavelty 2007, 67; Denning, 1991). ARPANET was tested amongst academic and government institutions in order to foster research and communications in the hope that it could create an effective communication system for the military (Cavelty, 2007). Security was not a primary concern, with a flexible and open approach being taken to early network protocol design. At this time, system vulnerability, insecurity and illegal hacking into corporate and governmental networks was unthinkable. The military domain has played a 'vital part in forging the link between modern information infrastructure and national security over the last 50 years' (Nagyfejeo, 2015: 152). Early computers played a 'considerable role in breaking military code systems during World War 2' (Nagyfejeo, 2015: 152).

Thereafter, during the Cold War, cryptography, the design of nuclear weapons and high-powered computing advanced hand-in-hand, signified by the acceleration of companies like IBM, Northrop and Cray (Cavelty 2007: 42; Hinsley and Stripp, 2001). In terms of the difference between previous and current cyber threat debate, however, it should be noted that information technology (IT) has served as 'a force facilitator or multiplier rather than a source of vulnerability in the past. Therefore, there was no desire to treat cyber threats as a national security issue, per se, until the 1980s' (Cavelty 2007: 41, Nagyfejeo, 2015: 152).

Some U.S. military officials argue that the militarisation of cyberspace is no different from the case of the wireless telegraph (Lovett, 2015). Marconi, who developed the first successful long-distance wireless telegraph (now known as radio), first initiated talks with governments, armed and defence forces, the maritime sector, the national post and telecom authorities in Western Europe and later in the U.S. These regions then became the first customers of wireless vendors (Steinbock, 2003: 68). Marconi expected the wireless telegraph to have a military purpose that could be used to 'protect lives at sea by means of ship-to-shore communication' (Steinbock, 2003: 69). As a result, Marconi is accredited with being the first person to wirelessly connect the Atlantic.

During the 20th century, the telegraph played a vital role in U.S. diplomacy (Steinbock, 2003; Berkowitz & Goodman, 1991). Following 'the development of Morse code, the telegraph became widely employed for military purposes in the U.S. Civil War' (Aid & Wiebes, 2013). From 1904 onwards, the U.S. Navy also began to introduce wireless telegraphy in order to communicate with its bases in the Caribbean

Sea (Aid & Wiebes, 2013). Shortly after, its significance became obvious the Congress empowered the President's control over the telegraph, telephone and marine cable in the U.S. in order to increase the power of the Executive in crisis (wartime) in a joint resolution in 1919 so that it could be operated accordingly during World War I. (U.S. Post Office Dep., Pub. Res. No. 38, 1921: 45).

Government circles all over the world soon began to use electronic communications for military and diplomatic purposes, capturing foreign communications without the communicators' knowledge due to vulnerabilities in the system (Aid & Wiebes, 2013). Consequently, this led to the development of 'signals intelligence' (SIGINT), which paradoxically caused the U.S. to realise that communications security (COMSEC) needed to be perfected (Sterling, 2008: 403). Accordingly, the U.S. developed more sophisticated methods and introduced electromechanical machines in order to encipher and decrypt messages (Bauer, 2002: 5).

1.5. Military leadership prioritises cyber offence over defence

Some argue, reductively, that the American concept of cyber war is irredeemably realist. Emphasising the physical security of the U.S. and the pursuit of national interests, some authors assert that the U.S. government's development of cyber offensive strategies leaves little doubt about the way in which the U.S. intends to militarise cyberspace to protect its own national interests (Mead, 2004). According to Retired Air Force General Michael Hayden (the former Director of both the CIA and NSA), the U.S. faces three different sources of cyber attack: (1) from states such as Iran or China; (2) from criminal gangs asking for money; (3) from unpredictable 'hacktivists' (Anonymous, LulzSec), who are considered the most alarming actors

since their intentions are unclear (Tadjdeh, 2013). Furthermore, it is also important to mention the vital role that the Internet plays in the radicalisation of fundamentalist ideas on social media sites, such as Facebook or YouTube, without the need for physical contact (Behr et al., 2013: 17). For instance, after publishing videos of its crimes online, the Islamic State (IS) managed to gain significant financial support and recruitment. In addition, Al-Qaeda maintains a number of websites in multiple languages that aim to disseminate propaganda to readers. For example, the websites detail instructions for joining Al-Qaeda, the depiction of imprisoned enemies' executions, and interviews with martyrs and suicide bombers (linked to Jihad against the West, and particularly the U.S.) (Jarvis et al., 2015: 19; Piper, 2008: 30). All of these issues are framed by U.S. policy makers as material problems that require action to be taken in cyberspace.

Despite insistence that the emphasis is placed on the defensive protection of its own computer networks, there has been an emerging consensus amongst high-level military officials regarding the establishment of a strong offensive deterrent. Since the new programme "Plan X" was initiated by the Defence Advanced Research Projects Agency (DARPA) in October 2012, the Pentagon's cyber warriors have been equipped to use cyber weapons offensively to break into enemy computers (Gjelten, 2013). Spending in this area is significant, with the US Air Force secretary, Michael Donley, reporting a 2013 budget request of $4 billion to achieve 'cyberspace superiority' (US GPO, 2012). In addition, the Pentagon has requested greater spending on cyber operations ($26 billion over the next five years) aiming to form a 6,000-strong cyber force by 2016 (Hickie et al., 2014: 14).

Therefore, the flavour of official discussions is increasingly that of offensive realism, and certainly so for the vast realm that is the Pentagon. The Cyber Command (USCYBERCOM) was established in 2010 and is now the world's largest cyber-defence organisation. Its establishment indicates a militarised response to cyber threats that aims to unify the cyber sections of the US Army, US Air Force, US Marine Corps, and US Navy into one central command. The Cyber Command, which reports to the US Strategic Command (USSTRATCOM), plays a vital role in carrying out both defensive and offensive operations against possible attacks coming from cyberspace (Bamford, 2013).

According to Erin Rosenbach, the deputy assistant secretary of defence for cyber policy '[t]hrough an intense deliberative process, the [most senior] leadership in the department decided that we needed to make a significant investment in the people who would constitute the cyber force' (Pellerin, 2013, Nagyfejeo, 2015: 145). The use of the word 'force' is indicative. Some argue that the main goal is to recruit as many 'cyber warriors' as possible in order to defend the U.S., to support combatant commands and to defend DOD information networks (Harress, 2014). The European Union and most European countries, in contrast, do not publicly speak about the possession of substantial operational and offensive capabilities in this area (Cyber Intelligence Europe, 2014).

As Steven Chabinsky, the former head of the FBI's cyber intelligence section, observes: 'There's no way that we are going to win the cyber security effort on defence. We have to go on offense' (Gjelten 2013; Nagyfejeo, 2015: 157). In July

2011, the Pentagon launched its 'Strategy for Operating in Cyberspace', which emphasised the following themes:

- Given that cyber attacks have become a major concern for national security as well as a new tool in foreign policy, cyberspace will be treated as the fifth domain of warfare and considered in the same way as the domains of air, land, maritime and space.
- The US Department of Defence (DoD) will employ new defensive methods for dealing with cyber threats.
- Cooperation at national and international levels will be fortified.
- The DoD will focus on developing a pool of skilled personnel and technological innovations: the recruitment of cyber warriors. (Dep. of Defence, 2011)

Furthermore, the DoD's new cyber strategy (Dep. of Defence, 2015) represents a milestone in terms of transparency and openness about the application of offensive cyber weapons:

> There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests.
> (DoD, 2015: 5)

However, it has been that the strategy is lacking in terms of reference to the 'Cyber Pearl Harbor' alarmism threatening to destroy America (Farell, 2015).

1.6. Cyber warfare aspects of U.S. strategic cyber culture

Analogy – Arms control in cyberspace

Analogies serve as a valuable method for illustrating complex or unfamiliar concepts through the use of simpler ideas or examples (Cavelty, 2012: 119). Many scholars have attempted to analyse and understand cyber threats through the use of analogies linked to other relevant historical experiences (Karas, 2008). Whilst strategies for tackling biological warfare are supported by considerable experience, the same cannot be said for cyber attacks. Given that global players must confront the same issues (e.g. the complex nature of the problem and the need to react quickly to changing conditions), cyber warfare could be usefully analogised by biological warfare. Common features of biological and cyber warfare include: *viruses* (biological vs. computer); *weapons* (which require little investment and are easy to develop at small locations); *multifunctional nature* (could be used for offensive, defensive, civilian or commercial purposes); *force multiplier* (capacity in conventional military operations); *unpredictability* (due to the complex system in which these weapons operate, electronic vs. atmospheric environment, and human or computer network targets); and *secrecy and surprise* (difficulty involved in detecting the root source of the attack) (Koblentz & Mazanec, 2013: 419-427).

The *Biological and Toxin Weapon Convention* (BTWC), which opened for signature in 1972 and came into force in 1975, can be used as a possible analogy in this realm (BTWC, 1972). The BTWC was the first treaty to 'outlaw various kinds of weapons (to ban the development, possession, stockpiling, and transfer of biological and toxin agents and delivery systems intended for hostile purposes or armed conflict)' (Koblentz & Mazanec 2013: 430). Furthermore, the treaty was signed during the height of the Cold War détente period, when mistrust and suspicion was at a low ebb. Although the signatories could not agree on the verification measures, the main goal

of the treaty was to forbid biological warfare (BW) and to fortify rules against any initiative to develop, possess or use them (Friedman & Brown, 2014: 52; Koblentz & Mazanec 2013: 430). It is convincingly demonstrated by Koblentz that Russia managed to secretly increase BW capacities for decades whilst publicly declaring that they had been renounced (Koblentz, 2009: 143). In 2001, at the Fifth Review Conference, negotiations stopped regardless of the events of 9/11 due to the failure to establish monitoring and implementation standards. The U.S. was also disavowed from Ad Hoc Group negotiations (Tucker, 2002). In short, the BTWC has proven to be a failure.

Despite the failure of the BTWC treaty to confine the development of BW programmes, international norms are still considered to be one of the most important tools in addressing both BW and cyber threats (Koblentz & Mazanec, 2013). Unfortunately, however, general national security toolkits are not yet equipped to tackle biological or cyber weapons successfully. There are several reasons for this. Firstly, it is difficult to apply punishment as a tool of deterrence due to the uncertainty of efforts required to verify enemy programmes or to identify the root source of the attack. Secondly, cyber criminals will always have access to new software and hardware tools that can be used to exploit system vulnerabilities more quickly than they can be defended, which calls the very nature of defence into question.

Nevertheless, the U.S. military is clearly applying deterrence doctrines by boosting cyber offensive capabilities (e.g. the establishment of U.S. Cyber Command at Fort Meade) in order to persuade the enemy not to attack U.S. national interests, because it would be too expensive. It is clear that simply by virtue of having a large economy as

well as the world's most advanced military and technology, the U.S. is leading the way in shaping cyberspace behaviour. However, the advocacy of offensive cyber weapons may not be the most beneficial path for the U.S. in its pursuit of maintaining long-term global dominance, because its economy is highly dependent on computers and networks. Therefore, the U.S. may be self-harming in its drive to see a cyber arms race play out.

Cyber warfare presents a number of hazards. Firstly, if everyone is committed to the same protocols, then there is a greater risk of exposure to irreversible vulnerabilities. Therefore, cyber warfare is more profitable for adversaries yet potentially indiscriminate. Given this, there is the widely held counter-assumption in much of the literature that the digital world would be safer and more secure if any attack on civilians or critical infrastructures by cyber weapons are treated as illegitimate (Koblentz & Mazanec, 2013: 430). As noted earlier, the EU only speaks publicly about its defensive cyber capabilities, which demonstrates the difference between the strategic cultural mind-sets of the EU and the U.S. Furthermore, attitudes towards offensive activity vary widely across Europe at the state level.

From a strategic culture perspective, the U.S. military has established a strong presence in cyberspace, sharing the belief that national security is under threat and that the military is best equipped to tackle the issue. Therefore, it is widely assumed that the U.S. is 'deliberately' undertaking militarisation at the operational level as a result of its approach to national security. Here, cyberspace is perceived as a new military domain wherein the development of specific deterrence mechanisms is

considered crucial in order to tackle cyber criminals, terrorist networks and to protect the critical infrastructures on which society is hugely dependent (Bisson, 2014: 2).

However, theories on the approach taken by the U.S. – and the motivations underlying this approach – vary widely between authors. According to Bisson, there are three main reasons why the U.S. embraces the idea of militarising cyberspace.

Firstly, any type of attack on civilian infrastructures could have a direct and devastating effect on the 'military-industrial complex', which would reduce the power of the U.S. military both at home and abroad.

Secondly, cyber weapons can produce the same effects as traditional weapons, as demonstrated in the 'Farewell Dossier' during the Cold War, when a Trans-Siberian gas pipeline suddenly exploded in 1982 (Weiss, 1996). Many reports speculate that this was a counterintelligence response (deception operation) planned by the CIA in partnership with the FBI, The US Defence Department and NATO. It is claimed that they sold legally camouflaged 'modified products and contrived computer chips that found their ways into the Soviet military equipment, flawed turbines were installed on a gas pipeline', resulting in the alteration of pipeline pressure and, ultimately, in disaster (Weiss, 1996: 125; Bisson: 2014).

Thirdly, the argument that an attack on the military network would cause more significant damage than a kinetic attack has been raised by many, since this may cause the cessation of military services, endanger the lives of American soldiers due to false military orders, and cause delays in the delivery of supplies. This is especially

true during an era where obtaining swift access to the right information drives access to the latest weapon systems and is therefore a decisive factor in winning wars (Bisson, 2014).

Cavelty takes a more granular approach and argues that there are five empirical factors that play a vital role in the development of the U.S. cyber warfare approach and militarisation of cyberspace.

The first factor is related to the paradoxical situation in which the number of computer security professionals is rising alongside rising fear of their intent (i.e. criminal or malicious).

The second factor is the identification of 'cyber enemies', often Russia or China, which are often accused by the US of stealing information for business and national security purposes or of developing offensive capabilities that the U.S, believes must be matched.

The third factor is associated with the rise of "hacktivism", which advocates the idea that all information should be free and that mainstream citizen politics should increasingly welcome online protest. The Wikileaks case accelerated the cyber debate over protests, and it is not surprising that states place priority on the protection of information considered vital to national security or that could be considered politically embarrassing.

The fourth factor is linked to the usage of the term ‘cyber war’, which has become more frequent in both media and policy circles, as well as in popular fiction.

Finally, the fifth factor is associated with an event that transformed security in the cyber arena: public exposure to the Stuxnet virus in 2009. What differentiated Stuxnet from other types of criminal malware was that it did not steal information or turn infected computers into botnets, but instead specifically targeted the Symantec SCADA systems in charge of supervising industrial processes. Stuxnet also caused the delay of the Iranian nuclear programme (Cavelty, 2012: 207-112). Following this event, greater acceptance of cyber war being implemented in practice was witnessed and scepticism began to decline.

Whilst the U.S. is often widely criticised for militarising cyberspace, it should be noted that others such as Israel, Iran, South Korea, France, Denmark and the Netherlands are also in the process of equipping themselves with cyber offensive capabilities (Interview, 2015q). US officials argue that it is crucial that the U.S. does not ‘just stand by and wait idly’, since Russia, China and a number of other rival countries are now recruiting their own national cyber warriors (Interview, 2015q).

For instance, in a PLA publication entitled *The Science of Military Strategy,* China finally broke the silence and openly acknowledged its network attack capabilities, involvement in digital spying and allocation of specific units dedicated to waging war on computer networks (Ward, 2015). In 2014, the U.S. Justice Department successfully filed criminal charges against five Chinese military officials who were accused of hacking and conducting cyber espionage against numerous American

companies (e.g. Westinghouse and U.S. Steel) whilst working for the Chinese People's Liberation Army and for providing data useful to Chinese competitors (Williams, 2014). However, the United States' prioritisation of an offensive cyber stance is not only driven by the rising offensive capabilities of other countries.

The Estonian cyber attack of 2007 is often regarded as a wake-up call that made many countries realise the serious defence skills needed to be developed in the virtual arena. This event also triggered the proliferation of cyber armies, either operated by governments or independently, or both. For example, some of the most well-known cyber armies are the People's Liberation Army Unit 61398 of the Chinese Army (code-name: "Byzantine Candor") and the United States Cyber Command (USCYBERCOM), which was created in 2009. Others include Russia's shadow hacker network (Net NGOs), which is thought to have been in operation since 2003; the Israeli Defence Forces' Military Intelligence Unit 8200, created in 1952; and the Syrian Electronic Army, which was founded in 2011 (Skaar, 2014).

According to confidential American diplomatic cables released by WikiLeaks, it is suspected that 'Byzantine Candor' (SECRET//NOFORN 11/03/2008), considered by the Chinese government to be a state secret, has been in operation since 2002. This is detailed in the following excerpt:

"42. (S//NF) CTAD comment:
Since late 2002, USG organizations have been targeted with social-engineering online attacks by BC (Byzantine Candor) actors. BC, an intrusion subset of Byzantine Hades activity, is a series of related computer network intrusions affecting U.S. and foreign systems and is believed to originate from the PRC."
(Secret State 116943, NOFORN, E.O. 12958, NY Times, 02/11/2008, Wikileaks)

According to a three-year investigation documented in a Mandiant report, the APT1 is thought to be the second bureau of the People's Liberation Army (PLA), and it 'has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously' (Mandiant Report, 2013: 3).

2. Strategic/policy dimension of U.S. strategic cyber culture

2.1. Establishing norms of behaviour in cyberspace

This section explores the policy dimension of U.S. strategic cyber culture, following on from the discussion of the military dimension in the above section. Therefore, this chapter highlights the non-military dimensions of U.S. strategic cyber culture and its commitment to an open, free and secure Internet with peaceful terms driven by the State Department.

There is an assumption that due to the relative power and inherently competitive nature of U.S. international politics, the U.S. aims to maintain its dominant cyber power 'by blinding herself to the belief that everyone has the same value system, but in reality the concept of value changes from one nation to the other' (Interview, 2015r).

Moreover, according to the 2013 *Presidential Directive 20,* the U.S. is duty bound to provide assistance to allies under foreign cyber attack (Fischer, 2013). It is also reputed that Obama diplomats are strategically working towards the implementation of international behaviour norms in the context of cyberspace, aiming to establish

rules on what constitutes an act of war. According to Michael Daniel, the White House Cybersecurity Coordinator, the need for international norms regarding cyberspace behaviour is crucial. Indeed, in his speech at the Gartner Security and Risk Management Conference on the 23rd June 2014, Daniel asserted that:

> We are promoting norms of behaviour for states in cyberspace that respect fundamental freedoms of expression and association, respect intellectual property rights, build trust and reduce the risk of miscalculation and escalation among states, and protect individuals from arbitrary or unlawful interference with their privacy online.
>
> (Castelli, 2014)

It is argued, however, that since countries such as China and Russia promote different judicial systems, cultures, norms and values to the U.S., the United States' assumedly God-given heroism may not apply in cyberspace despite the U.S. State Department's promotion of American values in this arena (Interview, 2015r).

A good example of the above point is the case of Germany and the U.S. regarding the right to freedom of speech. In this case, the German Constitution (or 'Basic Law') outlines German people's constitutional rights, whilst it is primarily the amendments to the U.S. Constitution that depict American rights (Lundmark, 2000: 297). The right to freedom of speech - symbolic of the extent to which a state is democratic – is protected under the Fifth Article[11] of the German Constitution and the First Amendment[12] of the U.S. Constitution. However, whilst the German constitution

[11] Paragraph (1) of Article V of the German Constitution states: "Everyone has the right freely to express and to disseminate his opinion by speech, writing and pictures and freely to inform himself from generally accessible sources. Freedom of the press and freedom of reporting by radio and motion pictures are guaranteed. There shall be no censorship."

[12] U.S. Constitution, Bill of Rights, Amendment I. states: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of

guarantees the freedom of expression and press, it includes provisions forbidding hate speech, Nazi propaganda and Holocaust denial under paragraph 130(3) of the German Criminal Code. This requires that those who 'publicly or in a meeting approves of, denies or downplays an act committed under the rule of National Socialism' are accountable to up to five years in prison or a monetary fine (German Criminal Code, 1998). Accordingly, unlike the U.S. Constitution, Germany's strict legal prohibition of hate speech also applies to cyberspace. For instance, in 2012, Twitter blocked the account of a neo-Nazi group (considered illegal in Germany) upon the request of the German police to close it 'immediately and without opening a replacement account' (Connolly, 2012).

Sino-American cyber diplomacy

The recent developments in Sino-American cyber relations, when President Xi Jinping of China visited President Obama in September 2015, illustrate how the State Department is applying a "soft power tool" in order to influence others and achieve goals through persuasion and diplomacy. The U.S. government has always been vocal in its position against economic espionage and, therefore, President Xi Jinping's visit was a historical turning point in terms of both governments agreeing on not to engage in this activity (White House, 2015b). However, the question of whether serious action will follow the agreements remains.

Snowden's disclosures in June 2013 caused damage to the United States' strategy of protecting trade secrets and establishing international behaviour norms to guard against economic espionage. Since the disclosures revealed U.S. trade and

---

speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

diplomatic negotiators engaged in the ongoing collection of intelligence information on foreign companies and commercial sectors, the U.S. lost its credibility as a powerful establisher of norms (Gellman & Poitras, 2013). Despite this, President Obama, along with NSA Chief General Keith Alexander, denied the collection of such intelligence: 'We do not collect intelligence to provide a competitive advantage to U.S. companies or U.S. commercial sectors' (White House, 2014). However, President Obama and former NSA Director General Michael Hayden have also confirmed that it is acceptable to collect information for national security purposes, as demonstrated in the following statements:

> Our intelligence agencies will continue to gather information about the intentions of governments - as opposed to ordinary citizens - around the world, in the same way that the intelligence services of every other nation does.
>
> (White House, 2014)

> There are two differences between us and the Chinese. We're actually more sophisticated, and we're self-limited. We don't do industrial espionage (...) I say, you know, if I had to talk to the Chinese about it, I'd go to Beijing, and I'd sit across the table, which I have done, and I would begin the conversation, "Look, you spy, we spy, but you steal the wrong stuff".
>
> (Hujer & Stark, 2014)

Therefore, the United States' promotion of certain types of espionage over others became problematic (Fidler, 2015).

Many analysts share the perspective that in relation to China, there is little difference as to whether espionage is conducted in order to seek information for military, intelligence and national security purposes (political secrets) or to steal information for intellectual property and business reasons (Segal, 2015). It is clear that the U.S. has the biggest stake in terms of economic security (e.g. for the

protection of intellectual property), and that this is one of the reasons why the U.S. is so eager to establish norms regarding economic espionage online. It is currently vital for China to enhance its national imagine and power. However, since the line seems to be blurred between the public and private sector, this makes things more complicated given the presence of state-owned enterprises (Lewis, 2015). For example, China's PLA notes both traditional espionage and business-oriented cyber spying. A former legal representative of the NSA also confirms that 'China steals Intellectual Property (IP) from the U.S. in order to leap ahead in technology' (Interview, 2015n).

Similar to China, the Russian government has forged strong partnerships with 'proxy' companies that will not act against government interests (Lewis, 2015). Furthermore, China and Russia often advocate the fallacy of the private sector, whilst the Russian government in particular has been found willing to hire criminal gangs in order to collect information for both intelligence and business purposes. This makes attribution difficult. However, whilst Chinese companies share information with the government at no cost, Russian gangs and companies are paid to commit espionage for the government (Interview, 2015n).

It has been highlighted that the Chinese government has stated its opposition to online theft for many years, and that its current stance is nothing new (Goldsmith, 2015). Furthermore, one of the most vital aspects of the cyber security agreement is the provision of assistance in cybercrime investigations: 'requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating' (White House, 2015b). However, this commitment to assist in cybercrime

investigations is in sharp contrast with past Chinese behaviour, adhering to a non-response policy even in the most routine of cybercrime investigations such as credit card fraud (Knake, 2015).

This being said, pressure from the U.S. had led the Chinese government to quietly arrest a number of hackers in recent times. This indicates that China may be taking positive steps to act upon its agreements, according to the Washington Post and a number of other reports (Nakashima & Goldman, 2015). Furthermore, security journalist Brian Krebs argues that the Chinese government has already been found to make arrests due to pressure from the U.S. government in the past, indicating that China may be more focused on eradicating cybercrime than appearances suggest (Krebs, 2015). Furthermore, a report presented to Congress in February 2012, including a note from the Office of Inspector General for NASA, Paul K. Martin, states:

> As a result of an OIG investigation and lengthy international coordination efforts, a Chinese national was detained in December 2010 by Chinese authorities for violations of Chinese Administrative Law. This case resulted in the first confirmed detention of a Chinese national for hacking activity targeting U.S. Government agencies.
>
> (Martin, 2012)

Moreover, Krebs confirms the leading role of NASA investigators in cybercrime investigations over the past decade – including 3FN and McColo – in his book, *Spam Nation* (Krebs, 2014).

Application of international law

One of the big dilemmas related to the concept of cyberspace is whether it should be considered shared resource a '*res communis'* like the world's oceans. According to

the 1982 UN Convention on the Law of Sea, oceans are shared by all and considered the ‘common heritage of mankind’. In other words, no state has the authority to exercise sovereign control over oceans (Hollis, 2012: 5). It is, therefore, the lack of clarity on cyberspace as a ‘res communis’ that causes states to respond differently to cyber threats. If it is a ‘res communis’, international law has clear standards that could be followed by establishing norms on its sustainability and free development (Hollis, 2012: 8).

Essentially, states have proven their competence in controlling cyberspace behaviour despite initial arguments amongst scholars that cyberspace and sovereignty do not mix (Goldsmith & Wu, 2006). According to Hollis, the Great Firewall of China is a classic illustration of ‘architectural control’, whilst the ability to project force into cyberspace could be regarded as another example of how states can effectively control cyberspace behaviour (Hollis, 2012).

Lotrionte (2015) argues that cyber security in the global arena relates to the de-conflicting of different legal authorities of nation states, not to the protection of a global "commons", despite the fact that the Defense Department's 2010 Quadrennial Defense Review Report described cyberspace as a global commons. This being said, it is clear that the notion of the law of armed conflict’s applicability to cyberspace is not embraced by China and Russia.

The following example will illustrate the difficulty involved in applying international law to cyberspace. Following the 26th Australia-United States Ministerial

Consultations (AUSMIN) in 2011, both governments agreed that a cyber attack on either nation would invoke the ANZUS Treaty[13]:

> In the event of a cyber-attack that threatens the territorial integrity, political independence or security of either of our nations, Australia and the United States would consult together and determine appropriate options to address the threat… consult together whenever in the opinion of any of them the territorial integrity, political independence or security of any of the Parties is threatened in the Pacific.

However, since both the U.N. Charter and ANZUS treaty recognise the right of both parties to retaliate under threat, this is not the concern with regards to the agreement. Rather, the concern is focused on what type of conditions retaliation is considered acceptable (Sullivan, 2014). The modern world is highly vulnerable to the 'power of technology', since it has the capacity to target financial sectors, destroy critical infrastructures such as hospitals, and overthrow governments. Therefore, technology evidently brings challenges to international law and collaboration, such as defining what constitutes an armed attack and what would constitute an appropriate response to such an attack in cyberspace.

The Tallinn Manual can be regarded as crucial groundwork for transatlantic collaboration to counter military-related cyber threats, although it has not yet been officially adopted at the time of writing. The primary goal of the Manual – produced by a group of international law scholars who met in Tallinn, Estonia – was to provide principles (95 guidelines for governments) on how international law can be applied in the unique context of the Digital Age (Schmitt 2013). This legal document, published

[13] The Australia, New Zealand and United States Security Treaty, or ANZUS Treaty, was an agreement signed in 1951 to protect the security of the Pacific. Although the agreement has not been formally abrogated, the United States and New Zealand no longer maintain a security relationship (Source: U.S. Dep. of State, Office of the Historian)

in March 2013, indicates mutual points of reference for the conflicting and colliding U.S.–EU definitions of military-related cyber attacks (Bendiek 2014: 8). However, the Manual is not without contradictions. Firstly, it does not clearly define what kind of attack is considered an act of war. Furthermore, terrorists and cyber criminals are given room for interpretation if international law is expressly applicable to cyber war, accepting war as a norm in the virtual realm just as war is accepted as a norm in the physical realm. Additionally, no respective behavioural norms exist in the context of armed assault in cyberspace (Schmitt, 2013).

According to Squadron Leader Emma J. Lovett, the Australian legal exchange officer at the Pentagon, 'defence is a constantly changing field and we probably would not have been able to foresee a military response to something like 9/11 until it happened' (Georgetown Cyber Security Law Institute, 2015). Moreover, Lovett demystifies the idea that cyberspace is the lawless "Wild West" – an ungovernable domain of an unregulated conflict – claiming that the cyber domain does not present anything radically new in international conflict. However, it is acknowledged that neutrality, attribution and the identification of private actors continue to remain an obstacle (Interview, 2015s).

In contrast, Udo Helmbrecht, the executive director of the EU's ENISA, along with many other EU officials, disagrees with this concept and compares the Internet to the "Wild West: 'Everyone can do what they want. There is no control, no regulation… And the reason for this is: where is the governance structure?' (EurActiv, 2015a). The difficulty involved in creating common terms at the policy/strategy and legal levels

are therefore demonstrated in part by the divergence of perspectives between the cyber security officials of the U.S. and EU.

Additionally, Lovett believes that the law of war is treated as a "do-as-you-would-be-done-by" affair (which also explains why Abu Ghraib was so detrimental) and suggests that cyberspace should be treated the same way. Therefore, this suggests that everyone should abide by *jus in bello* (the right to conduct during war) (Lovett, 2015).

2.2. Cyber security becomes a foreign policy issue: From Reagan to Obama

In this section of the chapter, the cyber debates surrounding each U.S. president will be examined in order to continue with the exploration of the policy dimension of U.S. strategic cyber culture. Understanding the way in which cyber policies, strategies and debates have developed since the Reagan administration will provide a clearer picture of what the main policy priorities were at this time when dealing with cyber threats and what the differences were in terms of the of cyber-oriented strategic mind-set of each President.

Reagan - 1984

The Reagan administration, which introduced two computer security-related policy documents, marks the beginning of the U.S. cyber threat debate. These documents were as follows: (1) the Computer Security Act of 1987 (out of a fear of espionage against the federal agencies' computer data); and (2) the Computer Abuse Act of 1984/86 (designed to tackle the problem of computer crime) (Congress 1988; Griffith 1990; Cavelty 2007: 24). It was only during the early 1990s that US politicians,

military leaders and media analysts began referring to the possibility of an "electronic Pearl Harbor", 'weapons of mass destruction' and other 'cyber-geddon' scenarios, wherein Critical National Infrastructure (CNI) and core networks would be threatened by terrorists, hackers or rival states using digital weaponry. The USA Patriot Act defines critical infrastructure as:

> …systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
> (Pinkowski, 2008: 114)

Since the year of 1998 marked the rise of heated public hearing debates, this was the most important year in the context of understanding the numerous types of cyber threats emerging during this era (Cavelty, 2007: 25). This was also the year when 'cyber-terror' was mentioned for the first time at a public hearing and became the main slogan of discussion. However, since government officials had a poor understanding of cyber terrorism at this time, the term was ill-defined, thus hindering evocative debate. This vagueness was also manifested in the foreign policy farewell lecture given by Clinton at the University of Nebraska in 2000, in which he stated that: 'One of the biggest threats to the future is going to be cyber terrorism – people fooling with your computer networks, trying to shut down your phones, erase bank records, mess up airline schedules, do things to interrupt the fabric of life' (Bidgoli, 2004: 356; Cavelty 2007: 101).

Clinton – 1998

In essence, the Clinton administration recognised the fact that both state and non-state actors pose a threat to the American public and private infrastructures in cyberspace (Kirchner & Sperling, 2010: 192). Therefore, Clinton developed a strategic plan called the Presidential Commission on Critical Infrastructure Protection (PCCIP) in order to protect critical infrastructure whilst boosting the capacities of intelligence and law enforcement communities to fight cybercriminals (Lukasik 1998; Bendrath, 2001). Cavelty notes that the first major report identifying the need to protect critical infrastructures – as "an intrinsic and essential element of our security strategy" – was the 1998 US National Security Strategy (NSS) (Cavelty 2007: 96; Clinton, 1998).

Following the issuance of the Clinton Administration's Policy on Critical Infrastructure Protection: *Presidential Decision Directive 63* (PDD-63) – which advocated self-regulation for the private sector with federal government intervention only in the event of market failure – the National Infrastructure Protection Centre (NIPC) was created within the FBI (Porcedda, 2011: 42; Jensen, 2011). The establishment of the NIPC can be considered the first key indicator of the U.S. taking a voluntary or self-regulatory approach in response to fear of 'big government' overregulation. The only exception was Public Key Cryptography, wherein the U.S. Government intervened (unsuccessfully) in an effort to maintain the long-standing convention of government dominance in the realm of secret communication.

Exemplifying the backdoor issue, it was in 1993 that the Clinton administration introduced the "Clipper Chip" – an encryption chip for digital voice communications. At this time, encryption was primarily only used by private networks and the

government: the World Wide Web was not really in existence, and the Internet as we know it today was in its infancy.

During the 1990s, the common American encryption standard was the IBM-developed Data Encryption Standard (DES), first created two decades earlier in partnership with the National Bureau of Standards (now the National Institute of Standards and Technology (NIST)) (Gallagher, 2015). Since DES was widely used by the financial industry and the development of commercial encryption started to increase, the government feared that criminals could exploit it and "go rogue". Therefore, in order to prevent this from happening, the Clipper Chip was announced. The Clipper Chip was based on the National Security Agency's (NSA) 1980s "Skipjack" encryption algorithm (as it was still classified in 1993). The key feature of the chip was key escrow, which could theoretically help the government to intercept any conversation from any point as long as people were using the Clipper device. In order to achieve this, all other encryption should have been banned. The White House officially abandoned the project in 1994 after the Clipper Chip failed to achieve the desired acceptance (Gallagher, 2015).

Furthermore, it is also important to note the PDD-63's acknowledgement of economic security as a national security issue, highlighting that the U.S. represents both the 'world's strongest military and largest national economy' and is simultaneously greatly reliant on the 'critical infrastructures and upon cyber-based information systems' (PDD-63, 1998). Consequently, the directive encouraged closer cooperation between the public and private sector in order to be better equipped against non-traditional attacks coming from cyberspace. It achieved this by considering each

sector of the economy and the government equally significant, claiming that 'critical sectors of the economy are hugely dependent on information technologies such as banking and finance, energy distribution networks and transportation system'. Therefore, any measures taken towards the elimination of vulnerability in the critical infrastructures (including cyber systems) should be a priority (PDD-63, 1998; Kirchner & Sperling, 2010).

Bush – Post 9/11

By the end of the 1990s, it was concluded that whilst terrorists and cybercriminals seemed the most likely to launch attacks, it was states who posed the greatest threat as a result of their capabilities. This point is emphasised by (Defence Intelligence Agency (DIA) director, Vice Admiral Thomas R. Wilson:

> Foreign states have the greatest attack potential (in terms of resources and capabilities), but the most immediate and serious threat today is from insiders, terrorists, criminals, and other small groups or individuals carrying out well-coordinated strikes against selected critical nodes.
> (Wilson, 2002)

However, despite the reverberations of 9/11, the focus on cyber terrorists was only temporary. Richard Clarke, former national coordinator for security, infrastructure protection, and counter-terrorism for the United States, also agreed that the US Government considers nation states to be a greater threat than the terrorists, stating: "There are terrorist groups that are interested [in conducting cyber attacks]. We now know that al Qaeda was interested. But the real major threat is from the information-warfare brigade or squadron of five or six countries" (Bendrath, 2004; Cavelty, 2007: 29; Nagyfejeo, 2015: 153-154). These assertions and consequent measures taken by the US government illuminate the way the US responds to cybercrime, depending on the motivation of the threat. Specifically, a profit-oriented cybercrime is met with

little interference and the expectation of a private sector response, whilst state-on-state attacks are met with a different kind of response.

Whilst the events of 9/11 did not generally result in a 360-degree turn regarding the strategy, they certainly made the U.S. aware of the possibility of terrorists attacking and damaging critical infrastructures, as well as the vital need to strengthen the nation's physical protections. This realisation is demonstrated in two executive orders signed by Bush (Executive Order 13228, entitled *Establishing the Office of Homeland Security and the Homeland Security* and Executive Order 13231, entitled *Critical Infrastructure Protection in the Information Age*), which resulted in the establishment of the Office of Cyberdefence at the White House and the President's Critical Infrastructure Protection Board (Bush, G.W., 2001b; Bush, G.W., 2001c).

Furthermore, according to Kirchner and Sperling, 9/11 presented a 'double-edged threat'. On the one hand, network-centric warfare played a vital role in the modernisation of the American armed forces. However, policy makers came to realise that information warfare could erase these advantages. On the other hand, the vulnerability of society and the state to mass disruption was recognised in line with acknowledgement of the government and public's dependency on cyberspace-related infrastructures (Kirchner & Sperling, 2010; Dep. of Justice, 2003).

Since cyberspace has no boundaries and is associated with a low level of entry for successful attack, the Bush administration also became aware that it cannot be considered easily defendable. As a consequence, the USA Patriot Act was extended not just to critical infrastructures, but also to national memorials and emblems that

were considered ‘symbolically equated with traditional values and institutions or U.S. political and economic power’ (White House, 2003: viii-xii).

It is also important to note that despite the Bush administration’s recognition of the vulnerability of the private sector, it contended that resources were not sufficient enough to protect industry and, therefore, governed along the ‘principle of subsidiarity’ (Kirchner & Sperling, 2010: 194). In other words, whilst the government was taking care of federal networks and information systems, industry was left to handle things ‘alone’, responsible for protecting private and public information systems (White House, 2003: 11). This was confirmed in the 2007 Comprehensive National Cybersecurity Initiative (CNCI), which sought to integrate the cyber defence policies of the military, law enforcement and (counter) intelligence but remained classified (White House, 2009: 4).

Cavelty argues that although Bush continued the fundamentals of Clinton’s policy strategy, laid down in the PCCIP, overall responsibility was given to the Office of Homeland Security to defend national critical infrastructures against terrorist attacks (Cavelty, 2007: 26). This shift in emphasis was subject to various criticisms, and the Bush administration’s ability to strengthen the level of critical infrastructural protection was questioned even further following the resignation of Amit Yoran, the government’s first cyber security chief, after just a year serving the National Cyber Security Division of the US Department of Homeland Security (McFadyen, 2008: 332). Speculation has arisen that the lack of prominence and attention given to his division within the organisation caused frustration that prompted his sudden departure (BBC, 2004).

Overall, it could be maintained that the Bush administration was less enthusiastic about cyber-threats compared to its precursor. This implies that the issue of cyber security and the protection of infrastructures were strictly linked and integrated into the physical aspects of terrorism by continuing a general discussion on the best strategy to counter terrorism and defend the country. Nevertheless, one of the weaknesses has been the disregard for the lack of apparent evidence of any actor having had the capacity to inflict serious damage to U.S. national security by exploiting the loopholes of automated information systems. Effectively, it can be argued that, driven by fear of terrorists taking strategic advantage of U.S. vulnerabilities, the government rushed into concluding that cyber terrorism was inevitable in its official statements (Cavelty 2007: 103).

Obama – After 2008

Obama's rejection of the Bush administration's approach to cybercrime can be seen in the proposed *Cybersecurity Act of 2009,* which claims that 'America's failure to protect cyberspace is one of the most urgent national security problems facing the country (U.S. Congress, 2009). The *2009 Cyberspace Policy Review* (CPR) highlighted that over the last 15 years, the administration was unsuccessful in determining the seriousness and complexity of the threat (White House, 2009).

Accordingly, the administration also recognised four major areas of focus:

(1) Failure of critical infrastructures (e.g. air traffic control systems or electricity grids)
(2) Cyber warfare
(3) Intellectual property theft
(4) Disruption or potential collapse of global financial system

(White House, 2009; Rollins & Henning, 2009).

The establishment of a 'cyber security policy official', responsible for reporting directly to the President, collaborate on policy framework with the National Security Council, and service as a member of the White House staff, was also promoted in the CPR (Kirchner & Sperling, 2010: 194).

Two additional innovations can be linked to Obama's cyber security strategy. Firstly, conversely to Bush, the strategy clearly states that the federal government takes responsibility not only for the cyber infrastructure of the state and local governments, but also of the private sector (White House, 2009). This indicates that U.S. economic security strongly supports the survival of the state and that it is also an issue of national security. It also acknowledges that 'the public and private sectors' interests are intertwined, with a shared responsibility for ensuring a secure, reliable infrastructure' (White House, 2009: vi).

Secondly, in order to tackle cyber security challenges, the administration emphasises the need to set up 'acceptable norms regarding territorial jurisdiction, sovereign responsibility, and the use of force' (White House, 2009). Furthermore, it also promotes legal frameworks, enhanced capacity to fight against cybercrime, common cyber security practices and standards as a way of institutionalising international collaboration on cyber security (White House, 2009: 21). Increased funding for cyber security, to the sum of $50 million in the 2010 fiscal year, represents another vital difference between the approach adopted by Bush and that of Obama. This marked 'a

fivefold increase over the annual amount budgeted during the Bush administration' (Kirchner & Sperling, 2010: 194).

3. Legal dimension of U.S. strategic cyber culture

3.1. The road from criminal law to cybercrime law

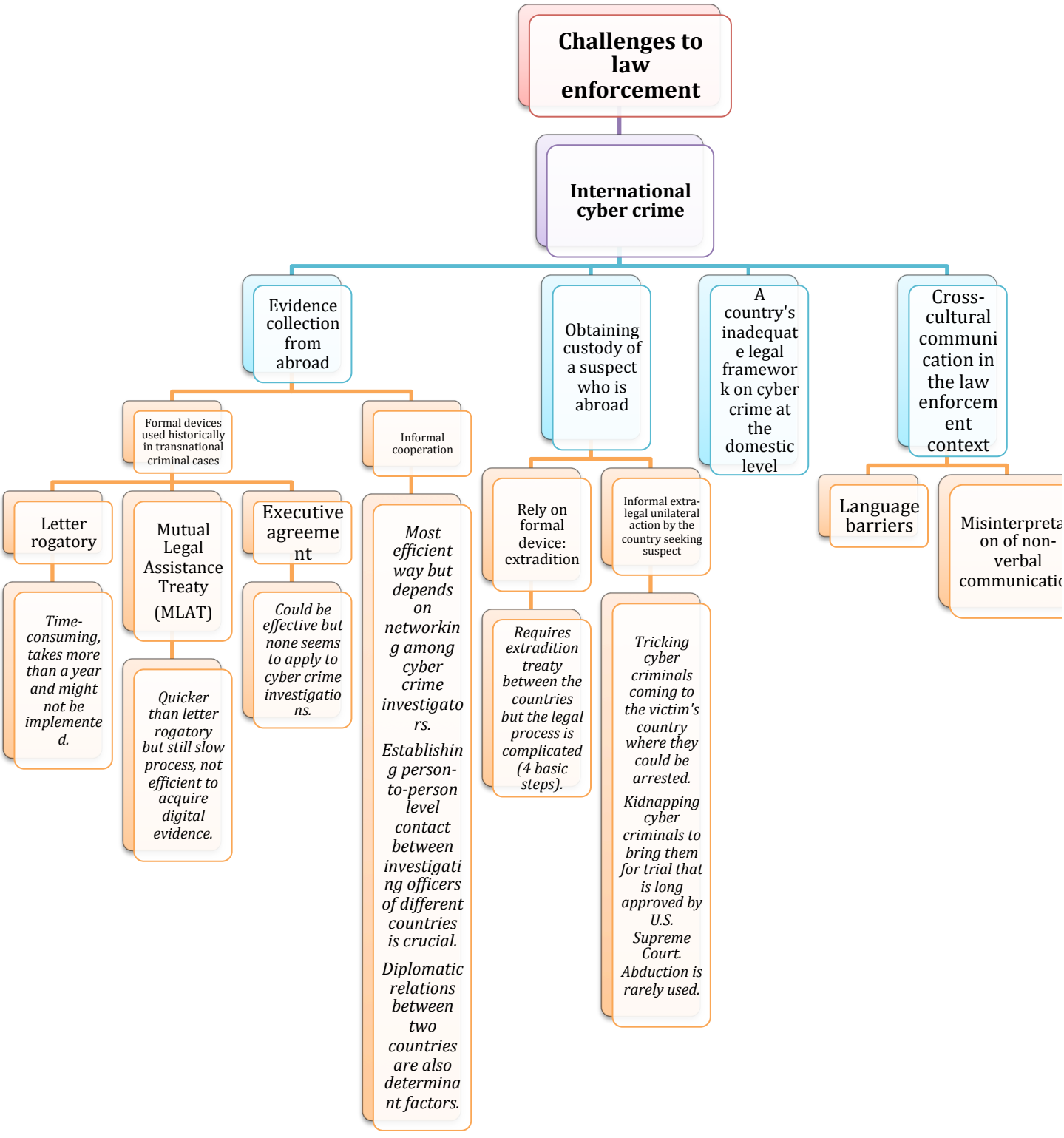
It is essential to analyse the development of U.S. criminal law as a representative of national legal culture in order to better understand the challenges involved in the cybercrime context of U.S. strategic cyber culture. One might observe that both the United States and the EU are highly legalistic entities and that the nature of their legal conceptions of cyber are central to the concerns of this thesis.

The "borderless" nature of cybercrime poses several challenges for prosecutors. There is a wide consensus amongst law enforcement officers that *transnational cybercrime* represents the greatest challenge that must be faced over future years (LEAP2015 Conference, Europol). Since the powers of police agencies are circumscribed by the territory and the nation state in which they are located, the task of law enforcement becomes vastly complicated when prosecuting those who commit transnational cybercrime. In other words, neither the FBI nor the German Federal Criminal Police Office have the legal right to even conduct preliminary investigations in foreign territory (Interview, 2015i). For instance, a German prosecutor can contact Google, but an FBI agent is not authorised to contact a German webpage provider (Interview, 2015i). It was also explained by the German prosecutor interviewed that due to special legislation, it is easier to collaborate in the case of war crimes than it is in the case of cybercrimes. This is despite the willingness of all parties to collaborate across borders. Effectively, this means that differences in national jurisdictions (e.g. issuance

of dual-criminality) prevents prosecutors and law enforcement from carrying out effective investigations.

In essence, each nation-state carries its own strategic cultural baggage, holding full legal authority over the territory it controls. Jurisdiction is one of the few areas that has not been impacted by globalisation, in contrast to the impact of regionalisation within the EU. Meanwhile, police officers are carrying out their tasks under a "sovereign" strategic culture (within a specific nation state), which makes it problematic to prosecute cyber criminals who are based in another nation state.

Therefore, it is widely argued that in the case of cybercrime prosecution, the time-honoured method of gathering evidence from abroad using formal device protocol is inadequate in this scenario. Moreover, whilst informal approaches to information-gathering seem to be a more efficient way of achieving collaboration between law enforcement officials, this is largely dependent on the investigating officer's social network and their expertise in contacting and cultivating counterparts in the country where the cybercrime has taken place. Therefore, whilst informal collaboration could well be considered an alternative mode for arresting cybercrime suspects, it is unlikely to be effective in all cases. Figure 4.4, below, outlines the complexity of enforcing the law in international cybercrime cases.



[Figure 4.4.]: *Challenges faced by law enforcement in the case of cybercrime*

Source: Based on U.S. Department of Justice, Criminal Resource Manual 274

Firstly, it is important to clarify that the U.S. is a federal government wherein 'sovereignty is divided constitutionally between the U.S. federal government (central governing authority) and the states (constituent political units)' (Sutton, 2002: 1-5). It can be said that the contemporary federal system is, in fact, the outcome of the U.S. Constitution that went into effect in 1789 (Brenner, 2010: 150). The drafters of the 1781 Articles of Confederation – the first constitution of the thirteen United States of America – were not in favour of a strong national government, for historical reasons (Schmidt *et al*., 2014: 36; Brenner, 2010: 150). The continued fear of a strong national government remains a distinct characteristic of U.S. strategic culture that can ultimately be explained by the colonists' experience with the British Crown's 'abuse of the criminal justice system to serve political ends' (Richman, 2005; Kurland, 1996: 21-25). Consequently, the authority of federal criminal law was largely disregarded and a significant portion of criminal law was represented at the local state level (Kurland, 1996).

Until the 20th century, Congress worked to locate the application of criminal law with the states, whilst 'criminal justice was overwhelmingly the business of the states, not the federal government' (Friedman, 1993:269). This began to change in 1910, when Congress started applying the Commerce Clause to criminalise certain activities, creating federal crimes (e.g. the transport of a woman/girl for prostitution in interstate commerce was considered to be a federal crime) (U.S. Supreme Court, 1913). Similarly, the transportation of stolen vehicles across state lines was criminalised at the federal level by the Dyer Act of 1919 and the Lindbergh Act (the Federal Kidnapping Act) of 1932 (Brickey, 1995: 1135). Consequently, by the end of the 20th

century, there had been immense development in federal criminal law and its enforcement (Friedman, 1994: 264-70).

Brenner argues that the introduction of technology (most notably the automobile) played a vital role in accelerating the power of federal criminal authority (Brenner, 2010: 152). This view is also shared by Brickey, who notes that 'laws like the Dyer Act were necessary because even though auto theft could be punished … under state criminal law, the jurisdiction where the theft occurred was powerless to pursue the thief across state lines … By crossing the state line, the thief could defy … local authorities' (Brickey, 1995: 1143). Therefore, Congress sought to address this problem by equipping the federal government with the power to prosecute offenders who exploited state boundaries via automobiles or other technologies in order to escape the prosecution of local authorities (Brenner, 2010: 152). Consequently, over 3,000 federal crimes were established by the turn of the 21st century (Myers, 2008: 1327).

Predictably, the extension of federal criminal law required the establishment of federal law enforcement agencies (Brenner, 2013). Until 1908, the Secret Service functioned as the only federal law enforcement agency when the Bureau of Investigation was created as part of the U.S. Department of Justice (DoJ). However, gaining greater investigative authority in line with federal criminal law, it became the Federal Bureau of Investigation (FBI) in 1935 (FBI History, 2003).

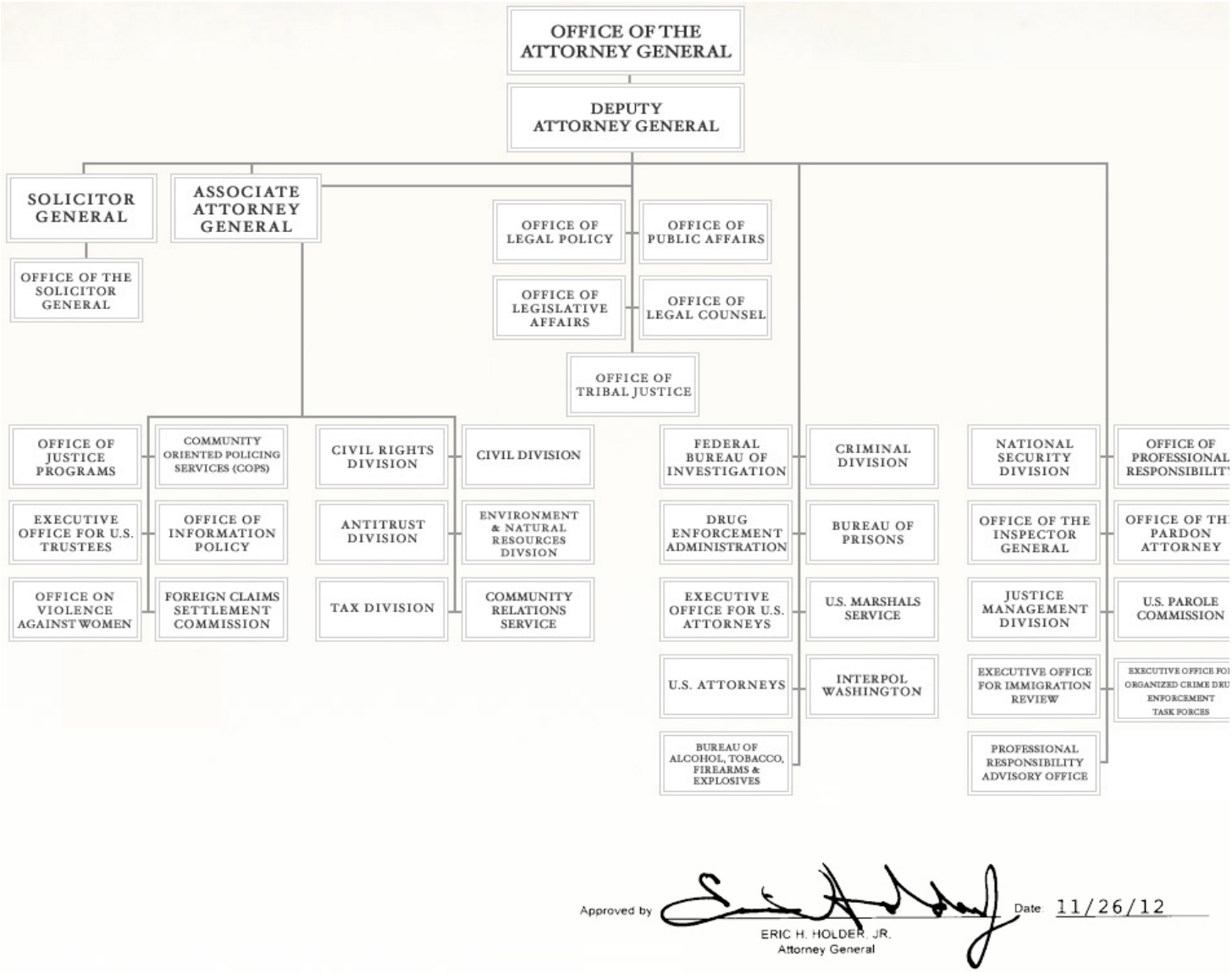
Alongside the FBI and Secret Service, further federal law enforcement agencies were also created, such as the Bureau of Alcohol, Tobacco and Firearms (ATF) in 1968, the

Drug Enforcement Administration (DEA) in 1973, and the U.S. Immigration and Customs Enforcement (ICE) in 2002 (Brenner, 2010). However, despite the expansion of federal law enforcement agencies, the responsibility of dealing with crime is still primarily handled at the state level, where state and local agencies are divided into three categories: state police, county (sheriff) and local/municipal police (Nadelmann, 2010). Importantly, it should be noted that the majority of cybercrime is dispersed at the local level.

When crimes committed in the U.S. are investigated by federal agencies, a common issue arises: coexisting jurisdiction between local, country and/or state agencies results in a complex negotiation process between the federal and state authorities in an attempt to determine which criminal cases should be dealt with at the federal or state level (Richman, 2000: 81). Since federal agencies have greater expertise, funding and time compared to state police; it is often the availability of resources that determine which party is allocated to a major criminal case (Richman, 2000: 94).

In the case of a criminal offence, a further complication is the determination of precisely what type of law (city ordinance, state statute or federal law) was violated, since local police do not pursue convictions for federal crimes and the FBI does not typically investigate or arrest individuals for state offences (Shinder, 2011). In essence, when a cybercrime is committed, the determination of geographic jurisdiction becomes one of the biggest obstacles, since the perpetrator is often not in the same city, county or country as the victim (Shinder, 2011).

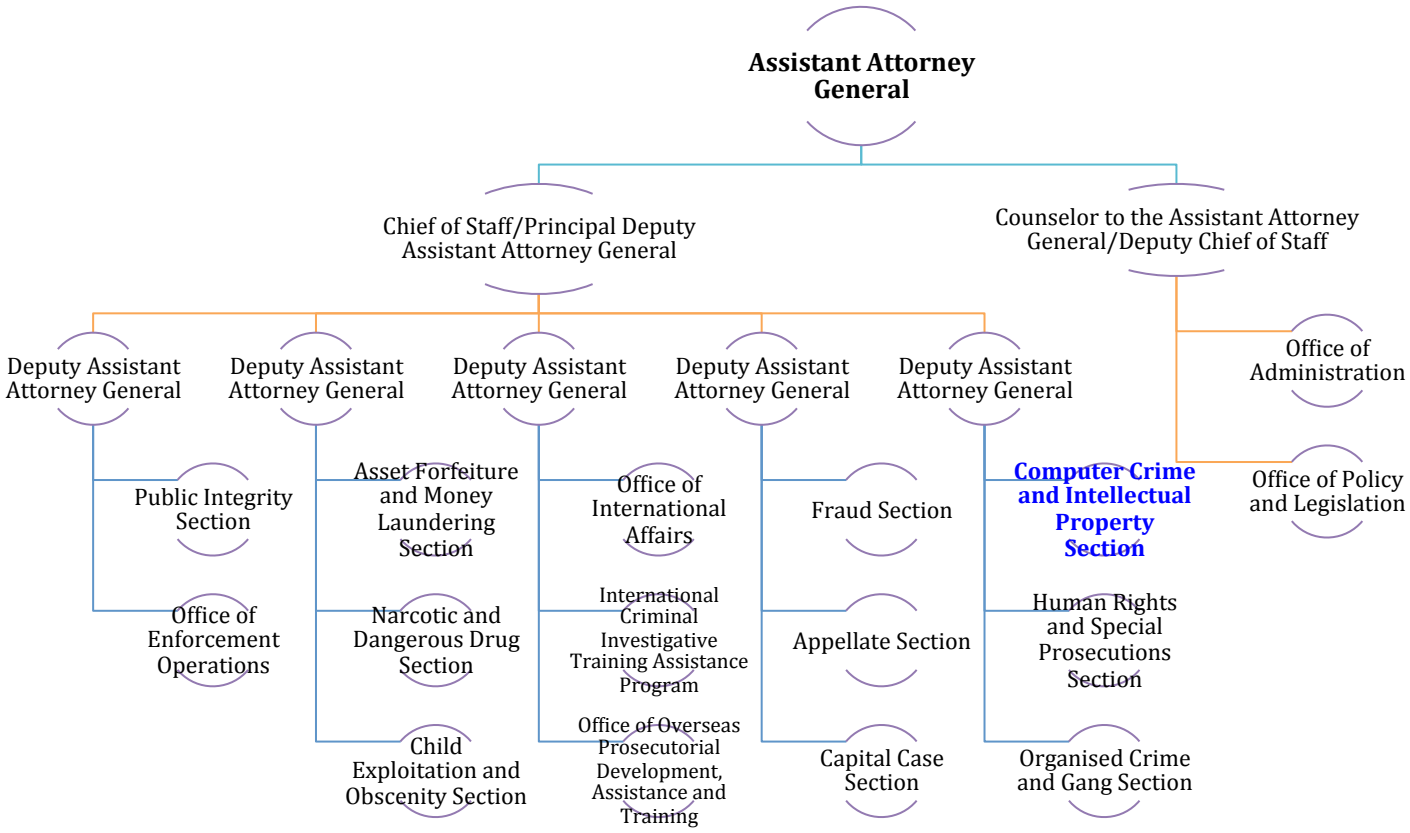
Moreover, the agencies in charge of prosecution often mirror the same bewildering divisions that we find within the law enforcement structure: U.S. prosecutors either work for a county prosecutor's office, in a state attorney general's office or for the U.S. Department of Justice (DoJ) (Brenner, 2010). Similarly, most crimes prosecuted by law enforcement agencies occur at the local level. This has been confirmed by an American Bar Association Study that concludes that in this realm, 'federal efforts account for only 5% of all prosecutions nationwide because the remaining 95% are state and local prosecutions' (Strazzella, 1998: 19).



[Figure 4.5.]: *Organisation Chart of the U.S. Department of Justice*

Source: Department of Justice, http://www.justice.gov/agencies/chart

As illustrated in the above Figure, the Attorney General is the head of the Department of Justice and holds authority over the appointed U.S. attorneys who carry out prosecutions in the specific geographical area - judicial district - allocated to them (Miller & Eisenstein, 2005). Next down the hierarchy are Assistant U.S. attorneys (AUSAs), who play a major role in a special Computer Hacking and Intellectual Property (CHIP) Program that began in 2001 that is designed to train cybercrime prosecutors (Brenner, 2010: 155). Over 260 CHIP AUSAs had been assigned to U.S. attorneys' offices by 2014, with at least one CHIP AUSA in each of the 94 offices dedicated especially to provide local federal level support to cybercrime prosecutors (Dep. of Justice, 2015a).



[Figure 4.6.]: *Organisational chart of the Criminal Division of the Department of Justice*

Source: Criminal Division of the Department of Justice, http://www.justice.gov/criminal

The Computer Crime Unit (renamed the Computer Crime and Intellectual Property Section (CCIPS) in 1996) was established by the DoJ in 1991 under the Criminal Division. The CCIPS is a specialist unit of cybercrime prosecutors working for the Attorney General rather than a U.S. attorney (Krotonski, 2015). Based on the above Figure, it is clear that AUSAs within the CCIPS report to a Deputy Assistant Attorney General who then communicates with the Assistant Attorney General. One of the main tasks of the CCIPS is to concentrate on the national and international aspects of cybercrime: something that is elaborated on in the U.S. Attorney's Manual, which emphasises that the CCIPS enjoys 'primary responsibility for developing the Department's overall computer and intellectual property offense enforcement strategies … and for coordinating computer crime and intellectual property investigations and cases that may significantly impact more than one district and/or other countries' (Dep. of Justice, 2015). Therefore, it is the CCIPS AUSAs who develop U.S. law and policy in the fight against cybercrime whilst engaging with officials from other countries in order to carry out investigations and resolve the limitations that exist between the legal systems of the two countries. Consequently, the cybercrime law of the CCIPS' counterpart eventually shifts in line with U.S. law (Brenner, 2010: 155).

Additionally, in December 2014, the Criminal Division created a new Cybersecurity Unit within the CCIPS that, according to Assistant Attorney General Leslie R. Caldwell, helps 'to create actionable guidance and to support public and private sector cyber security efforts' (Caldwell, 2015). The CCIPS is a unit that enjoys a flexible facilitating role, its only restriction being that it must comply with both domestic and

international law (Interview, 2016a). In other words, the unit is flexible as long as it adheres to the legal framework. As one senior US official remarked: "This new unit will strive to ensure that the advancing cyber security legislation is shaped to most effectively protect our nation's computer networks and individual victims from cyber attacks" (Caldwell, 2014).

The DoJ and FBI's encouragement of private sector collaboration in reporting cyber attacks and responding appropriate is demonstrated in the creation of the new Cybersecurity Unit. However, the private sector's residual resistance to government interference, fear of reputation damage, potential hesitance to share information, and lack of trust represent a significant issue. The Snowden revelations increased the divide between the White House and Silicon Valley, with both the Obama administration and FBI calling on Silicon Valley technologists to permit the creation of backdoors into encrypted mobile operating systems such as Apple iOS and Google Android (Gartner Security Summit, 2015).

Police culture is another major difference between the U.S. and EU, presenting a significant challenge in terms of collaboration against cybercrime. In the U.S., police culture has a long tradition of serving and protecting the community – representing *community* enforcement - in a highly decentralised and local manner. In contrast, in Europe, the police represent an *administrative* enforcement that is more accountable to the government: in other words, a "police for the rule of the government" (Interview, 2015t).

Thus, crime has long been – and still remains – a local matter, from a cultural perspective. The current U.S. law enforcement system has evolved from a system that worked well before the introduction of modern transportation (e.g. automobiles) and technology. Much like the 1930s, when gangsters managed to escape the local police by automobile and prosecution by jurisdiction, cyber criminals reap the rewards that technology and the Internet provide (Milner, 2003: 135).

In response to the challenges generated by automobiles for the local police, federal law enforcement started to expand its authority. Today, law enforcement is in a similar situation, challenged by a new set of technologies. However, cyber technology has had much more profound effects, and the prosecution process has become more complex. Today's cyber criminals can commit crimes in multiple jurisdictions using the Internet, just as yesterday's criminals could commit crimes in multiple jurisdictions using the automobile. Thus, technology has created, as Brenner says, 'a virtual world that overlays with the physical world' (Brenner, 2010: 156).

Accordingly, whilst the traditional capture of offenders travelling between states was complicated, the virtual environment now makes it even more difficult and complex to track down offenders. A cyber criminal who launches cyber attacks against a U.S. victim could be located anywhere in the physical world. Parallel challenges include the acquisition of digital evidence that is different to the "physical" evidence that police officers and prosecutors are accustomed to dealing with. If officers are untrained in cybercrime, there may also be the risk of digital evidence being overlooked or even damaged (Casey, 2011: 26-27; Reyes et al., 2011: 11).

According to Brenner, problems can be also linked to insufficient training offered to state and local law enforcement officers. This is, in turn, driven by several factors. The first factor is that teaching the basics of digital evidence gathering is expensive (Brenner, 2010). The second factor is related to the method of training used: it is suggested that prosecutors should be trained along with the police, ensuring that prosecutors comprehend the way in which digital evidence could be used in court (Interview, 2015m). The third factor is the frequent re-training of officers and prosecutors in order to ensure that they are able to keep up with rapid technological developments and, consequently, cyber criminals (Georgetown, 2015).

Digital evidence, unlike physical evidence such as fingerprints or DNA is not a "fixed" or unchanging verification, but one that is constantly evolving and requires sufficient investment by law enforcement into new equipment in order to keep pace (Clancy, 2011: 87). Furthermore, the private sector's failure to file police reports is an obstacle often raised amongst police officers (Georgetown, 2015). For instance, if the victim calls the bank first and the bank takes immediate action (e.g. reimbursing the victim), the victim will rarely think to report the crime to the police (Interview,, 2015m).

Since cyber security is a field characterised by rapid innovation, there is a wide consensus that 100% security will never be achieved in this domain. Additionally, it is always going to be a challenge for law enforcement agencies and prosecutors to acquire the same technological advancement as cyber criminals. Accordingly, significant differences are seen in the budgetary allowances of U.S. police and prosecutors' offices, resulting in different resource and training capacities, much like

in the EU. Funding has also changed at the centre, depending on whether the administration is republican or democratic (Interview, 2015t).

Law enforcement agencies are competing with other areas of government, typically the military, at all levels for funds for training and cybercrime investigation purposes (Reyes et al., 2007: 11). EU agencies such as ENISA and Europol are also struggling with the same issue, with an officer at ENISA explaining that EU agencies' budgets are also largely dependent on how close a relationship they have with EU decision makers (Chatham House, 2014).

When requesting funding for cybercrime investigations and training, this is often in addition to the funds already allocated to the law enforcement agencies and prosecutors' offices for routine crime (Interview, 2016b). For instance, according to the Department of Justice FY2014 Budget Request, there is a $668 million budget for cyber resources, designed to tackle 'computer intrusions and cybercrimes and defend the security of the Department's critical information networks' (Dep. of Justice, 2014b). This budget also includes an increase of $92.6 million to combat sophisticated cyber attacks (Dep. of Justice, 2014b). In terms of the FBI budget, an additional increase of $86.6 million has been requested in order to promote the 'FBI's Next Generation Cyber Initiative, which will more strategically focus the FBI's efforts on the greatest cyber threat intrusions into government and industry computer network' (Dep. of Justice, 2014d).

A change in law enforcement culture has been witnessed, partly as a consequence to the above points. Over the last few years, there has been a tendency on the part of

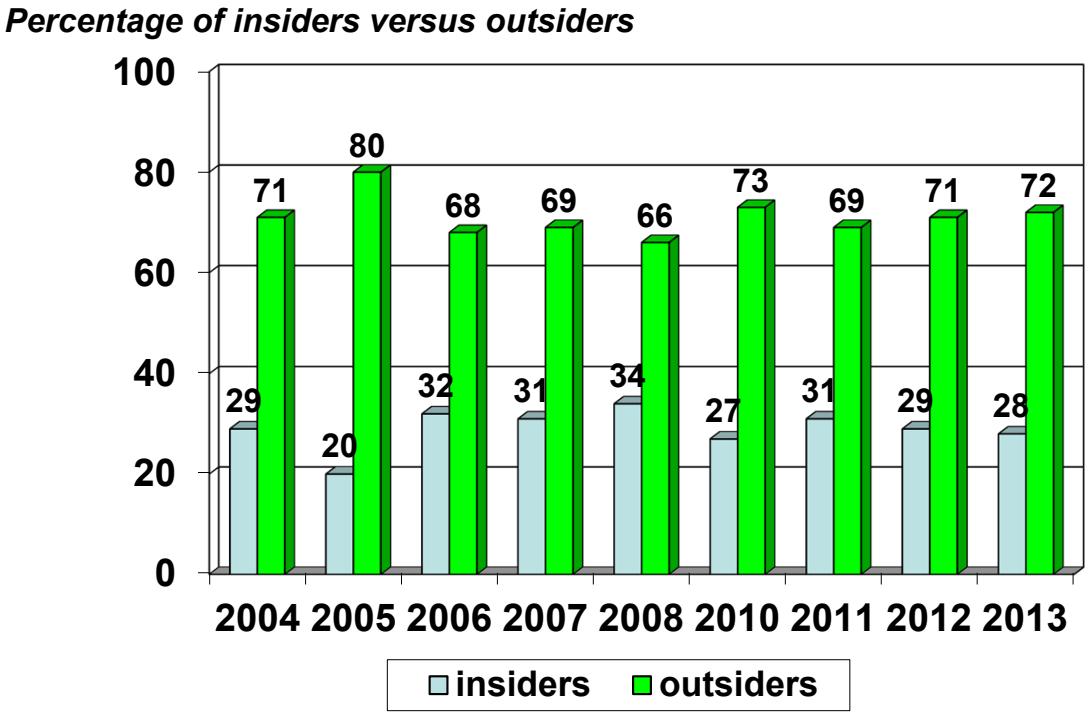
directors of law enforcement agencies such as Europol and FBI to move into the private sector. This phenomenon reflects a certain sense of disillusionment, since agencies and police units do not have sufficient resources or capacities to conduct effective cybercrime investigations in well-equipped forensic labs compared to firms such as Microsoft or PwC.

Predictably, budgetary competition in this rapidly changing area creates political tensions between agencies in the USA. The visceral nature of this situation was confirmed during the interviews with current and former officers from the NSA, FBI and DHS. Here, agencies' competition over budgets results in staff taking an attitude of keeping information to themselves and creating an 'uneasy' atmosphere. Interestingly, a former associate general counsel for Information Systems Security working for NSA and DHS confirmed that U.S. agencies trust each other less than they trust their European counterparts (Interview, 2015n). The NSA has achieved exceptionally effective collaboration with the GCHQ and, in parallel, the FBI has also developed strong relations with Europol.

3.2. Arrival of federal cybercrime laws: never-ending struggles

Before the era of computers and computer crimes, technology was used primarily to facilitate traditional crimes like theft (Interview, 2015u). In the early days, computer crime was largely conducted by authorised users called "insiders" who tried to manipulate computer programs (e.g. to steal money) (Brenner, 2010). In contrast, this phenomenon has moved dramatically in the opposite direction today. According to the PwC U.S. State of Cyber Crime Survey, directed by Carnegie Mellon University, only 28% of electronic crime events were carried out by "insiders" in 2014 (PwC,

2014). Figure 4.7, below, demonstrates that no more than 34% of cybercrimes were committed by insiders between 2004 and 2013, with crimes committed by outsiders reaching a high of 80% in 2005.



[Figure 4.7.]: *U.S. State of Cyber Crime Survey 2014*

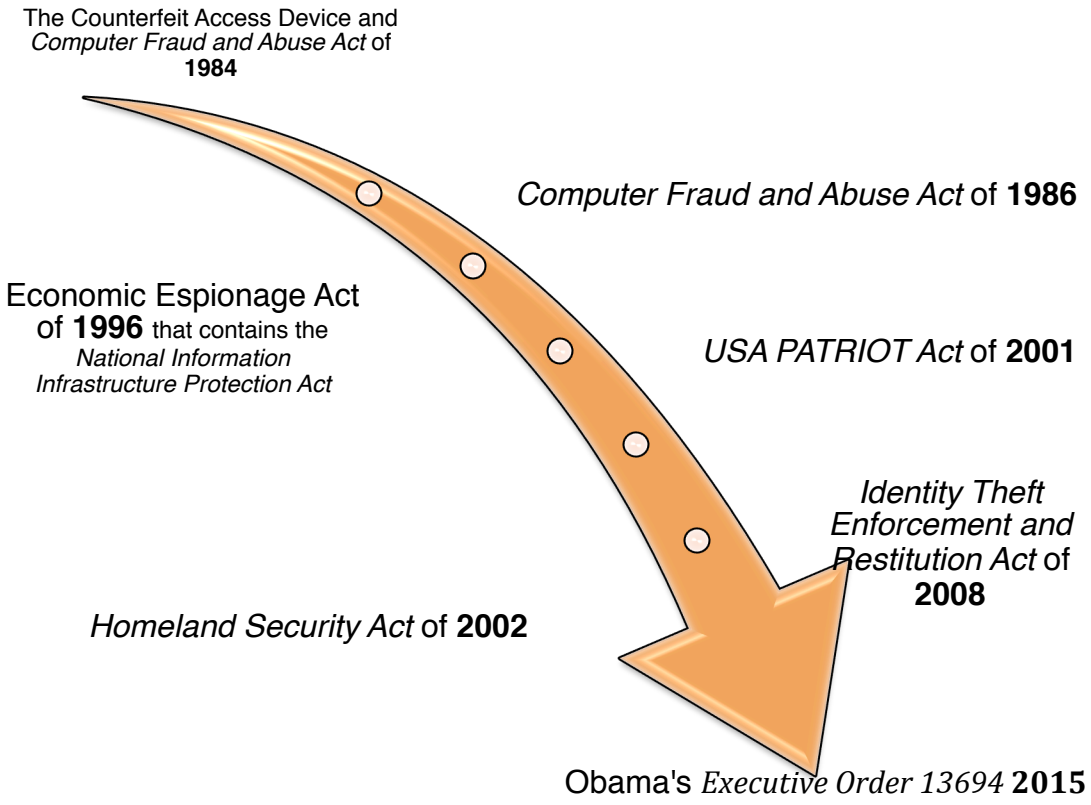
Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014

Judges were often required to deal with cyber criminals using traditional criminal law principles and procedures due to the lack of specialist computer crime law prosecutors (Schell & Martin, 2004). However, since traditional crime law did not apply to the unique criminal aspects of new technology, it quickly became evident that this approach was ineffective.

A useful illustration of the dilemma involved in the application of traditional criminal law to a cybercrime case is provided by former DoJ officer, Mark Rasch. A former employee (a defence contractor) who now works for a new company – a competitor – still has access to his previous computer account, which his previous employer never deleted. As a consequence, the former employee has the power to gain valuable information about his former company through his "undeleted" computer account and to share this information with the competitor for which he works, something that is considered highly valuable to the company (Interview, 2015u). However, the question arises as to whether the former employee has actually committed a criminal offence. Essentially, the difficult lies in whether the obtained information can be considered property, and whether it is therefore capable of being stolen. Additionally, if the former employee has access to his previous computer account and checks the phone directory (that is publicly available), is there a need for a "theft" prosecution warrant? In this, can permission for access be considered implicitly granted? (Interview, 2015u). Moreover, in order to be considered a criminal offence, must the criminal be aware of the confidentiality of the information?

Rasch argued, concerning criminalisation, that whenever a data breach occurs, there is still no legal clarification as to how to quantify the harm caused by the data breach (Interview, 2015u). Therefore, these dilemmas still pose as great a challenge to prosecutors today as they did a decade ago. The number of challenges involved in this area extend further than the ones outlined here and will be elaborated upon to a greater extent later in this chapter.

It has become apparent to prosecutors that the application of traditional law is clearly not the most efficient way to counter computer crimes. This has resulted in a call for new and specific laws to be implemented (see Figure 4.8). This is not a new phenomenon: the first federal computer crime law that aimed to protect federal government computers was the *Counterfeit Access Device and Computer Fraud Abuse Act* of 1984 (CFAA), which was passed by the Congress and amended in 1986 (Cavelty, 2008: 47). The difficulty involved in creating computer law lies in the fact that all other computer laws are an amended version of the CFFA – the most important U.S. computer crime statute (May & Practical, 2004: 1; Baker, 1993: 68).



[Figure 4.8.]: *Evolution of federal cybercrime jurisdiction and prosecution* (selected legislations)

It is important to note that the CFAA already links computer crime to national security, outlawing unapproved access to classified information in U.S. defence and foreign relations. This highlights the argument that national security is held at the core of the U.S. approach to specialist legislation, unlike the EU's approach (Cavelty, 2008: 47). For this reason, the US has also criminalised the inappropriate use of financial data from financial institutions and government businesses, empowering the Secret Service (the Treasury's police) to carry out investigations in parallel with the FBI (Sterling, 1993; Cavelty, 2008; Burke, 2001). As with any other agencies that carry out similar tasks, tensions between the FBI and the Secret Service were present even when the involvement of the Secret Service was minimal compared to the FBI (Cavelty, 2008).

However, since the CFAA focuses not on the way in which a computer is used but on the method of entry used to gain access to the computer (i.e. in order to prove unauthorised access), insiders note that there are limitations to the CFAA in that it does not necessarily enable insiders to be prosecuted (Adams, 1996). Additionally, since the CFAA does not criminalise the act of viewing data on a computer even if that information was obtained through unauthorised access, this represents another limitation that should be noted (May & Practical, 2004).

It was not until 1996, when the *National Information Infrastructure Act* (NIIA) was passed as part of the *Economic Espionage Act,* that U.S. law finally banned the theft of trade secrets in a way that included electronically stored information (Fischer, 2013). The NIIA was important in terms of expanding the CFAA, broadening the definition of a 'protected computer' to refer to any computer that was connected to

the Internet, and criminalising the unauthorised viewing of information on that computer (Drummond & McClendon, 2001; Cavelty, 2008).

Cybercrime was often treated as a national security issue by policy makers even in the early days, although perhaps less so during the 1980s than during the 1990s. Until 1993, cybercrime was strictly linked to digitally classified information and the 'theft thereof by means of computers' (Cavelty, 2008: 54). In other words, the main issue at this time was the threat of foreign intelligence. Policy makers then became concerned about the vulnerability of U.S. national security to foreign espionage as information technology became a greater part of people's daily lives during the late 1980s and early 1990s (Cavelty, 2008).

This national security mentality in the fight against cybercrime illuminates one of the most profound characteristics of U.S. strategic culture, as noted earlier in this chapter: to protect the preservation of the American way of life, liberty from external threats and the belief that the U.S. is the nation chosen by God, duty-bound to fight evil and bring 'light' to the world (Hampton, 2013: 32). In much the same spirit, the following quote from CFAA 1986 also demonstrates how computer crime was linked to the national security threat via the exploitation of classified information:

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government […] to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data […] with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation […] shall be punished.

(CFAA 1986 (US) 18 USC 1030 (a))

The above excerpt from the CFAA serves as the main basis for prosecution and highlights the clear relationship between national security and the protection of valuable information (Doyle, 2014).

In some part due to this national security framing, 9/11 could be regarded as a turning point in the history of U.S. federal cybercrime law. It was during that time that major changes were introduced, for the first time since the last amendment in 1996 and the revised CFAA (Cavelty, 2008: 104). The introduction of the 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act' (*USA PATRIOT Act)* - which became law on the 26th October, 2001 – played a vital role in helping to expand the government's power in parallel with law enforcement and intelligence agencies seeking to investigate terrorism (Swan, 2012: 61).

In the continuing absence of congressional action on cyber security information-sharing legislation, President Obama issued Presidential Executive Order 13636 'Improving Critical Infrastructure Cybersecurity' in February 2013, along with Presidential Policy Directive 21 (PPD 21), 'Critical Infrastructure Security and Resilience' (White House, 2013b; Nagyfejeo, 2015: 162). E.O 13636 addresses two vital issues: (1) advocating voluntary information sharing on cyber attacks between U.S. federal agencies and private sector critical infrastructure (CI) owner-operators; and (2) protecting privately-owned CI (Fischer et al., 2014; White House, 2013b). In addition, federal agencies are obliged to share 'unclassified reports of threats to U.S. companies in a timely manner' (EU Parliament, 2013; Nagyfejeo, 2015: 162). The

executive order has been deemed satisfactory by those who argue that E.O. 13636 represents necessary steps forward in securing essential and comprehensive cyber security legislation where there was previously a lack. Conversely, others have argued that the order does not differ significantly from existing processes and that there is a fear of government overregulation and inappropriate intervention in private sector activities (Fischer *et al*., 2014).

E.O. 13636 can be considered an amended version of the controversial H.R. 624 cyber-security bill, the Cyber Intelligence Sharing and Protection Act (CISPA), which was introduced in 2011 (Weiss, 2015: 13). In the event of a cyber attack, CISPA encourages private companies and the government to voluntarily share information. However, advocates of civil liberty and privacy argue that CISPA could erode civil freedoms because it does not specify privacy protections, whilst its proponents protest it could help to better identify cyber attacks. In April 2013, CISPA was passed by the House despite failing to be passed by the Senate in 2012. The act was reintroduced in Congress in 2013 but has since stalled (Nagyfejeo, 2015: 162).

Since the White House threatened to veto this divisive bill, new legislation was introduced by Senator Dianne Feinstein: the S. 2588 Cybersecurity Information Sharing Act (CISA). CISA was passed by the Senate Select Committee on Intelligence in July 2014. CISA uses similar language to CISPA, promoting the sharing of information between government agencies and the private sector; although, in contrast to CISPA, it does not oblige an entity to deliver information to the federal government (Weiss, 2015: 15). In December 2015 Obama signed CISA into law.

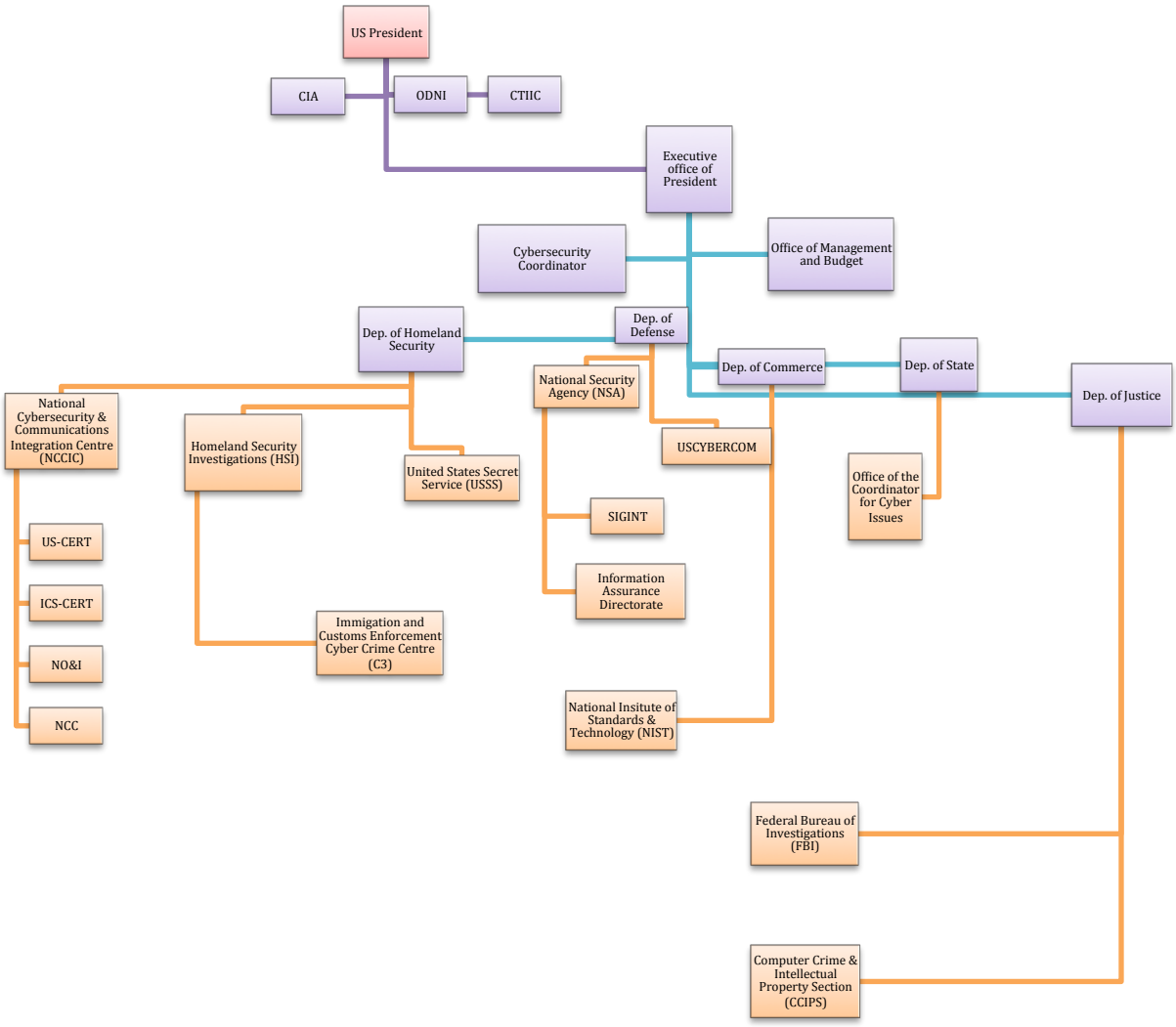
Accordingly, the 'Cybersecurity Framework for improving critical infrastructure cybersecurity' provided by the National Institute of Standards and Technology (NIST) runs in parallel with Executive Order 13636 (Nagyfejeo, 2015). This framework offers a technology-neutral approach based on voluntary consensus standards by focusing on the functions that an organisation is required in order to manage cybersecurity risks (US Department of Commerce, 2013). Furthermore, it consists of five functions (know, prevent, detect, respond, recover) and three levels of implementation (senior executive, business process manager and operational manager) (EU Parliament, 2013). The DHS has also helped to assist with the implementation of the framework by creating the Critical Infrastructure Cyber Community C3 Voluntary Program so that CI partners can better comprehend and engage with the framework (Dep. of Homeland Security, 2014).

4. Operational dimension of U.S. strategic cyber culture

The operational dimension of federal agencies' approaches to countering cybercrime – as another non-militaristic approach – will be outlined in this section of the chapter. As noted throughout this chapter, the U.S. demonstrates a disjointed approach to cybercrime at present. Generally speaking, the FBI, the U.S. Secret Service (USSS) and various others all deal with crimes that have high-tech elements. However, they each have their own individual agency-driven strategic cultures that determine their approaches and philosophies when dealing with cybercrime cases (see Figure 4.9, below).

As noted, there is huge competition between federal agencies, with the FBI considering itself the leader and actor with the greatest responsibility. Since no

precise official definition of cybercrime has been outlined by the U.S. government, nor any overarching national security strategy exclusively designed to tackle cybercrime, federal law enforcement agencies are essentially are left to their own devices. Consequently, cybercrime is defined based on the agency's specific definition during investigation (Finklea & Teohary, 2015: 15).



[Figure 4.9.]: *Washington D.C.-based overview of US federal structure*

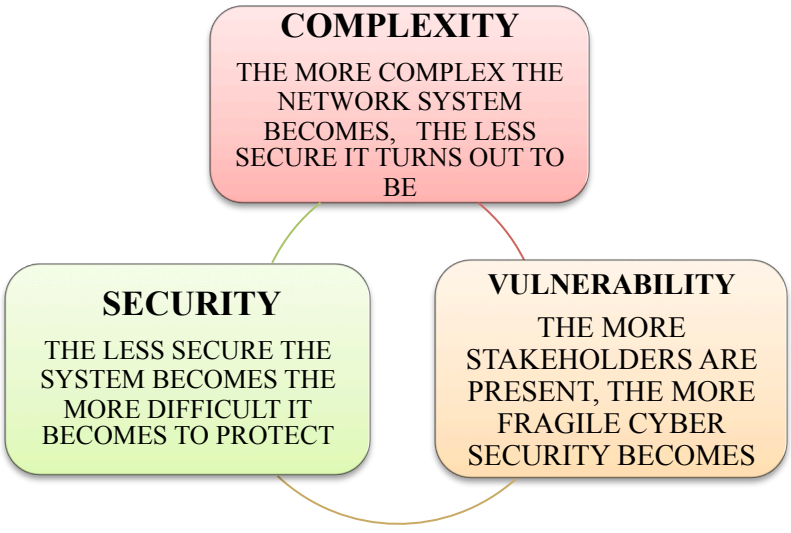
Source: Borrowed from RAND Europe, 2015

4.1. Battling the "unknowns" in cyberspace

In order to achieve success in cybercrime investigation, cyber security is often conceptualised in terms of business relationships (e.g. public-private or public-public) by law enforcement officials. The following points highlight the numerous challenges that law enforcement agencies such as the FBI must face.

a) Complexity

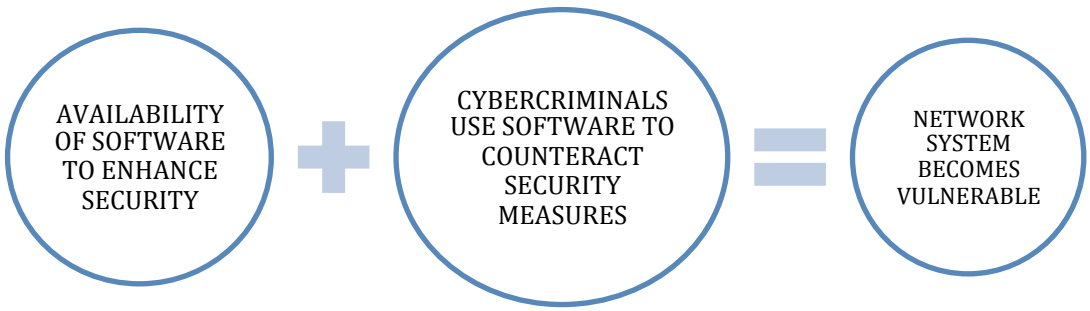
The underlying dilemma that now affects every layer of our society and causes profound problems for law enforcement is our dependence on the Internet. We are also focused on achieving the access and efficiency it offers whilst obtaining cost-savings. However, every time we reengineer a business process to increase efficiency, we increase the risks and open ourselves up to greater vulnerability (see Figure 4.10, below).



[Figure 4.10.]: *Complexity*

Complexity, according to Bruce Schneier, is the 'worst enemy of security' (Schneier, 2011). The more complex a system becomes, the more vulnerable it is. Today's computer systems can therefore be considered less secure now than they have been in the past, but more secure now than they will be in future years, due to the increasing complexity of modern computer and network systems. The paradox of the Internet is that the more fundamental and vital it becomes to our life, the more difficult it becomes to protect it. Therefore, there is an emerging need for the development of a coherent central system that can respond quickly and effectively to cyber security challenges. However, in reality, cyber security has no centre: instead, it is possessed by a diverse group of individual actors. Each of the large stakeholders owns a share of it (software vendors, ISPs, banks, police, and the central government), which runs the risk of a 'nightmare scenario' without a coherent cyber security plan being put into place. In short, the more stakeholders that are present in cyber security, the more fragile and difficult the system becomes. The private sector is considered cyberspace's biggest stakeholder, since it holds 85% of U.S. critical infrastructures and key resources (e.g. PwC possesses its own in-house IT forensic laboratory) (Rice *et al*., 2011: 3).

b) Endless availability of new technologies



[Figure 4.11.]: *Endless series of vulnerabilities of the network system*

Security technologies are not developing particularly quickly. Therefore, the Internet becomes ever more difficult to protect. However, it is not only the lagged development of security technologies that cause the vulnerability of the system. The paradox originates in the availability of software and hardware tools that are designed to enhance Internet security measures. Owing to their availability, cyber criminals can use them straight away to counteract these measures (Peiravi, 2010: 15; Flammini *et al*., 2013). Furthermore, the Internet allows entry to the cyber security market at a low cost that favours cyber criminals. Since we depend so heavily on the Internet and submit such a wealth of personal information into it, this makes theft and hacking an increasingly tempting option that is increasingly likely to severely interrupt our daily lives. It is also strongly related to the infringement of privacy, meaning that stricter security measures are needed. In response to this, the FBI has attempted to develop both its own attitude and 'philosophy' towards cyber threats as well as its own policy.

4.2. FBI Cyber Division

Since its creation in 2002, the Cyber Division of the FBI has undergone tremendous changes and is currently taking the lead within DoJ. As the online environment moves through continuous change, the Cyber Division has had to respond similarly in order to deal with the emergence of issues such as IP rights violations and online child exploitation.

The FBI therefore plays a dual role in tackling cybercrime. Firstly, the FBI considers dealing with cybercrime either as a criminal element or a nation-state actor: in other words, the FBI serves as a domestic intelligence agency whose main priority is the

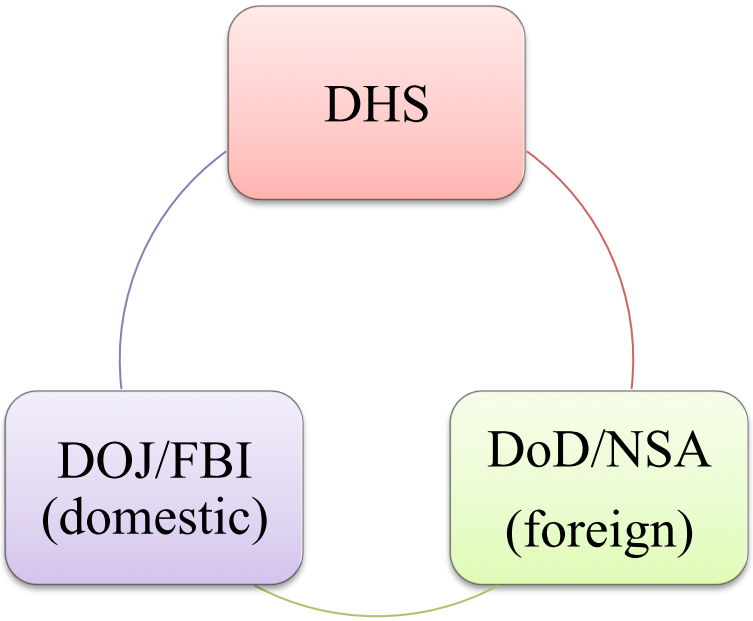
protection national security. The FBI's other role is associated with its influence on the enforcement of U.S. federal laws as the key law enforcement agency of the nation. Both the FBI and the USSS share jurisdiction over investigations that concern 'violations of the Computer Fraud and Abuse Act with regard to cyber intrusions into protected systems' (Doyle, 2014; Van der Meulen, 2015: 71).

Furthermore, the FBI's cybercrime investigations follow a twofold response method, depending on the motivation and intention of the cybercrime: that is, whether the crime was motivated by profit or by state-against-state conflict. In other words, the FBI deals with not only criminal matters but also with national security authorities. Consequently, the FBI is tasked with handling both basic hacking activity (e.g. attributable to an individual criminal attempting to, say, hack into a bank account) and national-scale espionage activity targeting intellectual property or the U.S. government (Interview, 2016b). At times, the optimal realistic goal is to temporarily disturb criminal activity, although the ultimate goal is to achieve criminal conviction. According to Lemieux, if the case is a profit-oriented cybercrime, states such as the U.S. prefer not to interfere too heavily, instead expecting a response from the private sector (Interview, 2015t).

The DHS is responsible for remediation and protection, helping victims to address the consequences of the crime and recover after a cyber attack whilst the often FBI investigates it (Interview, 2015q). In other words, the main mission of the DHS is civil safety. Additionally, the FBI-led National Cyber Investigative Joint Task Force (NCIJTF) also plays an important role by bringing together 19 U.S. agencies and Five Eyes partners from both the law enforcement and intelligence community in order to

synchronise their investigation methods in the cyber field. Over the last few years, the NCIJTF has become into a maximising and harmonising international power that is capable of carrying out investigations against cyber adversaries (Quinn, 2014).

To recap, despite the fact that the intelligence, law enforcement and civil safety community share the same goals, their approaches and priorities are clearly different. In effect, every federal agency/community has its own strategic culture, and each agency's specific strategic cyber culture governs their response to cyber threats (see Figure 4.12, below). The respective roles of the various agencies are also depicted in Table 4.2.



[Figure 4.12.]: *Responsibilities of federal agencies fighting cyber crime*

[Table 4.2.]: *Summary of Agency Roles*

DHS	DoJ/FBI	DoD/NSA
▪ Coordinate the national protection, prevention, mitigation of	▪ Investigate, attribute, disrupt and prosecute cybercrime	▪ Defend the nation from attacks ▪ Gather foreign

and recovery from cyber events ▪ Disseminate domestic cyber threat and vulnerability analysis ▪ Protect critical infrastructure ▪ Secure federal civilian systems ▪ Investigate cybercrime under DHS' jurisdiction	▪ Lead domestic national security operations ▪ Conduct domestic collection, analysis and dissemination of cyber threat intelligence ▪ Support the national protection, prevention, mitigation of, and recovery from cyber incidents ▪ Coordinate cyber threat investigations	cyber threat intelligence to determine attribution ▪ Support the national protection, prevention, mitigation or, and recovery from cyber incidents ▪ Investigate cybercrime under military jurisdiction ▪ Protect the country from cyber warfare

Source: Based on Donald J. Good's presentation (deputy assistant director of the FBI's cyber operations), ITBN Conference, September 2015

Since the organisational cultures of each agency differ, it is the sharing of classified information that has the most significant impact: 'The systems of these agencies were not designed to share classified information, only if there is a mutual legal agreement' (Interview, 2014c). In other words, nation-states are still considered legal entities, which explains why bilateral cooperation is often prioritised over multilateral cooperation. Moreover, the presence of bureaucratic competition and threat of losing control over their data means that many agencies – even at a national level – prefer not to exchange information with one another. This could be the reason for the disjointed U.S. response to cyber threats. Despite the lack of trust between federal agencies on the nation level, however, better collaboration is often achieved between the U.S. and its European counterparts (e.g. the FBI with Europol, NATO with the MoD, and Europol with Interpol) (Interview, 2015n).

4.3. United States Secret Service

Originally, the USSS was granted investigative power 30 years ago, when the Computer Fraud and Abuse Act was created in supported of the endorsement of the Comprehensive Crime Control Act of 1984 (Van der Meulen et al., 2015: 69). Under this law, Congress authorised the USSS to inspect criminal offences related to illegal access gained to computers as well as the fraudulent use, or trafficking of, access devices (Van der Meulen et al., 2015: 69). Proactive investigations often grant the USSS the advantage of being the first to expose a potential or existing cyber-related security breach, according to the testimony of Deputy Special Agent William Noonan of the USSS' Cyber Crimes Division (Noonan, 2014). This is also followed by the swift notification of potential victims (e.g. financial institutions or organisations) in order to help mitigate the damage caused by the security breach and to stop the criminal from gaining unauthorised access to the victim's network. The USSS partners with the local US attorney's office in order to launch a criminal investigation once the owner of the compromised system has confirmed that unauthorised access has been gained (Van der Meulen et al., 2015: 70). On the plus side, an effective partnership is maintained with both national and international partners in transnational cybercrime investigations, especially when it comes to the application of Mutual Legal Assistance Treaties (MLATs) with the support of the State Department and DoJ, as well as with the European counterparts (USSS agents are allocated at both Europol and Interpol) (Interview, 2016c). However, the DHS' failure to respect the USSS' authority to enforce legislation is a common complaint (Interview, 2016c).

Under the aegis of DHS, the USSS also maintains close collaboration with the Immigration and Customs Enforcement Cyber Crimes Center (C3). C3 was

established in 1997 with the purpose of 'delivering computer and cyber-based technical services in support of ICE's Homeland Security Investigations (HSI) cases' (Van der Meulen et al., 2015: 70).

4.4. The role of NIST

Whilst the NSA is responsible for national security systems, NIST provides federal governments and agencies with guidance and security standards for non-national systems. Some argue that compared to the EU, the U.S. approach and cyber security framework are more voluntary in nature (Interview, 2015v).

The Cybersecurity Framework (labelled Version 1.0) stems from Executive Order 13636, directed NIST to develop a framework for working with the private sector. A year was spent engaging with industry, with a public request for information input broadcast through six workshops in collaboration with the academic sector. Effectively, it was this long collaborative process that truly helped shape the framework in terms of rebalancing whether 'it would be too high level, ineffective and kind of impractical or too low level, detailed and prescriptive where it couldn't be used either' (Interview, 2015v). The reason utility is emphasised is that it is meant to apply to all 16 sectors defined by NIST as critical sectors, subsectors and sub-subsections of U.S. infrastructure.

NIST was also tasked with reviewing a series of global international standards that could be utilised across the different sectors. Subsequently, NIST identified five international standards that would work well in different applications across the field. Organisations are free to adopt any internal processes or standards they prefer since

NIST hopes to offer companies flexibility in terms of input (Interview, 2015v). At present, different organisations are subject to different framework outcomes. For example, fairly unsophisticated SMEs may use the framework for guidance when planning a risk management strategy. For more sophisticated organisations (global and multinational companies), the framework offers formats that facilitate more complex mapping of their internal practices. Many of the companies use a 'mix-and-match' approach, selecting the elements of the framework that best suit their needs.

Certain business lines may use bespoke standards: for instance, special 'internal practices' that do not exist in the codex, are often used by highly sophisticated organisations. However, they still map this into the framework and use it for gap identification in order to measure whether they have overinvested (not just underinvested) in certain areas. It is also used as a communication tool to express how different business lines within the organisation manage cyber security risks. Furthermore, NIST frameworks can be deployed internally and externally between organisations and through some third-party relationships in the supply chain or with business partners in order to demonstrate how partners are managing cyber risks (Interview, 2015v).

One NIST official observed that whilst developing the Cybersecurity Framework, one of the industry requirements was to ensure that whatever framework NIST developed would be complementary to, and able to function effectively in, the global marketplace. Since NIST already advocated international standards, this was not an issue. Since then, NIST has studied the approaches taken to this issue in other countries and markets. NIST has also been working on advocating a more voluntary

approach tailored to specific market needs. Comparing the EU and NIST approaches, it is clear that the U.S. is adopting more of a 'grass roots' approach, whilst the EU is advocating a more top-down approach to the management of cybercrime.

5. Conclusion

Compared to the EU, it can be said that the U.S. boasts a longer history with regards to cyber security. In reviewing this trajectory, this dissertation asserted that due to unique differences in the United States' approach to cybercrime at the operational and policy/legal levels, the U.S. should not be considered a single monolithic entity with regards to cybercrime and cyber security. Furthermore, it is clear from the discussions outlined in this chapter that due to the range and variety of policy implementations in existence, there have been many intersecting mandates – typically between the DHS and the FBI – which have improved cooperation greatly over the last 18 months, according to the Review Commission.

However, whilst significant improvements have been demonstrated in counterterrorism collaboration, the area of cyber security has witnessed slower developments. This can be explained by the lack of clarity between the various roles and responsibilities at the U.S. national level. Since there is no official leading investigative agency in the case of cybercrime, a division of labour (based on the competences of the various agencies) exists. Whilst the DHS (USSS) and the FBI are currently responsible for cybercrime aspects, the NSA and DoD (USCYBERCROM) are the main experts on military aspects (such as cyber defence and offence) in practice. Furthermore, this chapter has demonstrated the conflict between the conceptions of these against and those focused on cybercrime.

Additionally, the previous chapter examined the amalgam of contradictory approaches found amongst the U.S. federal agencies (FBI, DHS, DoD and ICE) when dealing with cybercrime at all three levels. This demonstrates that the U.S. is too large to command a single strategic cyber culture. Instead, U.S. strategic cyber culture is comprised of both militaristic and non-militaristic compounds that, together, form a rather fragmented national cyber culture.

Despite the fragmented nature of the strategic cyber cultures present in both the EU and the U.S., the significance of transnational cooperation has been recognised at both the strategic and operational levels. The U.S. example suggests that the involvement of several institutions and entities (approximately 62 federal offices) in the area of cyber security make an already complex landscape even more complicated through the creation of overlapping mandates. Thus, the allocation of respective responsibilities can become an issue of concern when cybercrime activity does arise. This implies that the EU may need to exercise caution when creating new bodies or overlapping mandates amongst existing bodies.

Chapter V.

Finding the "golden" balance between privacy, cyber security and surveillance Case study: Blackshades

'We as a people have not yet created a consensus as to what it is we want our government to do… or what we will permit our government to do in order to protect us in the cyber domain.'
(former CIA and NSA Chief General Michael Hayden, August 2015)

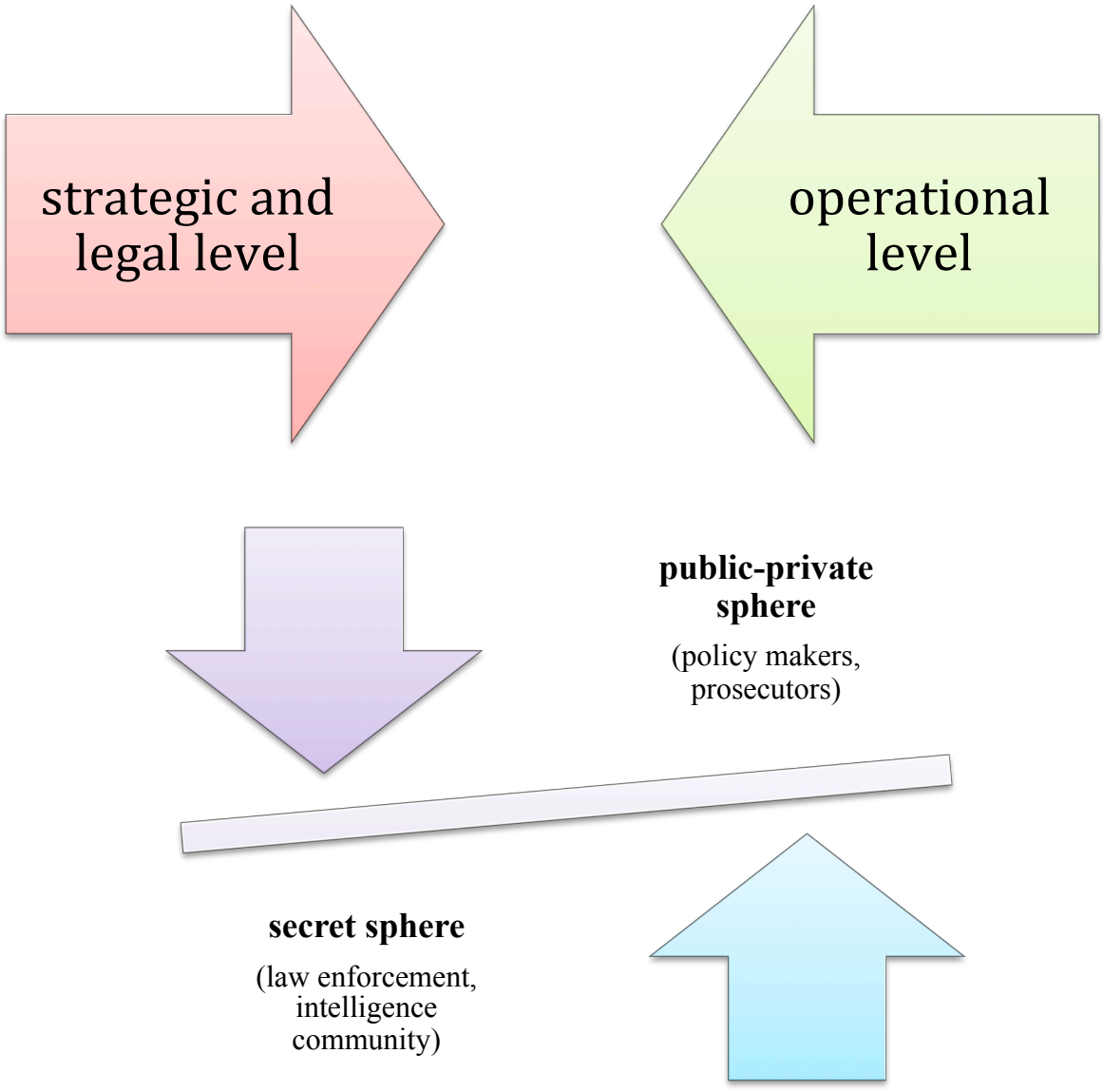
Fighting cybercrime effectively is beyond the capacity of any single nation state. This activity thus requires international collaboration that exceeds state-to-state partnerships and includes the private sector. Despite differences in the areas of law, privacy, strategies and technical standards, the EU and the U.S. face a similar cyber threat landscape, one in which they cannot ignore the crucial role of private stakeholders. This is because the private sector owns most of the relevant data that could be used as evidence in the prosecution of cyber criminals and also support the development of strategic responses, especially for law enforcement agencies. To demonstrate, Europol has already been endeavouring to establish strategic partnerships with private partners through the signing of the 'Memoranda of Understanding' and by appointing representatives to participate in the EC3's advisory groups (internet security, financial services, and now a third group for communication providers). In addition, Europol has established the EC3 Academic Advisory Network (EC3AA), inviting the academic community to participate in this important issue (Europol, 2015b). It is clear that, more than ever; cybercrime needs to be dealt with at a multi-stakeholder level since the Internet permeates our society more completely day by day.

To a certain degree, it is ultimately *technology* rather than policy or law that will dictate the parameters of the cyber domain. In particular, the advancement of privacy conscious communication tools such as end-to-end encryption for calls and email content (whereby only the recipient can decrypt a message) created by companies such as Google or WhatsApp now frequently cause problems for the intelligence and law enforcement community in their attempts to effectively track down criminals and terrorists (Greenberg, 2014).

This chapter proposes that there are fundamental differences in how the EU and the U.S. fight cybercrime and what they deem to be appropriate measures in this context on both a strategic and legal level. This research explores the proposition that various cyber cultures are present in both the U.S. and in the EU and that these cultures influence transatlantic collaboration at different levels. Therefore, as already suggested, it might be overly simplistic to claim that, for instance, the U.S. perspective on cyber space is informed solely by military concerns when in reality this approach is merely the view of the Department of Defence (USCYBERCOM) and stands in notable contrast to the approaches taken by other branches of the U.S. government (e.g. the Department of State, the DoJ and the DHS). Similarly, we might be careful to label the EU as having one single strategic cyber culture when different approaches are present on various levels, whether it is in the public-private sphere, the agency sphere, the legal sphere or the secret sphere. Additionally, one must remember that the EU is made up of 28 Member States, each with their own mind-set and historical baggage.

This thesis therefore suggests that divergences on the policy and legal levels are indeed relevant and create a 'strategic dissonance' when prosecuting cyber criminals. However, this is in sharp contrast to the convergence and efficiency of collaboration at the operational/executive/security services level (see figure 5.1.).

Could there ever be harmony and interconnectivity between the working procedures of these two different spheres?



[Figure 5.1.]: *Challenges of collaboration at various layers in the fight against cybercrime*

We also need to reflect on the question of whether a *corporate* solution – public-private partnership - could be the answer to the cyber security problem. Corporate giants such as Microsoft (99,000 full-time employees in 2013) and Google (53,600 full-time employees in 2014) have a huge amount of resources available to them in the form of technical expertise, data and scale of research budget. They are thus far more prepared to tackle cybercrime than agencies such as GCHQ, which has only 6,100 employees – moreover they are already transnational entities used to working seamlessly across borders (Hopkins & Harding, 2013; Statista, 2015). Therefore, the superiority and influence of the cyber security culture of giant companies needs to be taken into account in the context of transatlantic cyber security collaboration that suggests a mosaic-like, decentralised strategic cyber culture.

In the aftermath of the Snowden disclosures in 2013, U.S. technology companies have become less inclined to collaborate with foreign intelligence agencies. This has manifested itself most obviously in the addition of encryption software and the requirement of a U.S. federal court order to enforce a request for disclosure (Interview, 2015f). Robert Hannigan, who became the director of GCHQ in 2014, wrote an article in the *Financial Times* arguing that GCHQ along with its sister agencies are unable to face the challenges of cybercrime without the support of the private sector, especially the large U.S. tech giants who are the major players in the cyber domain (Hannigan, 2014).

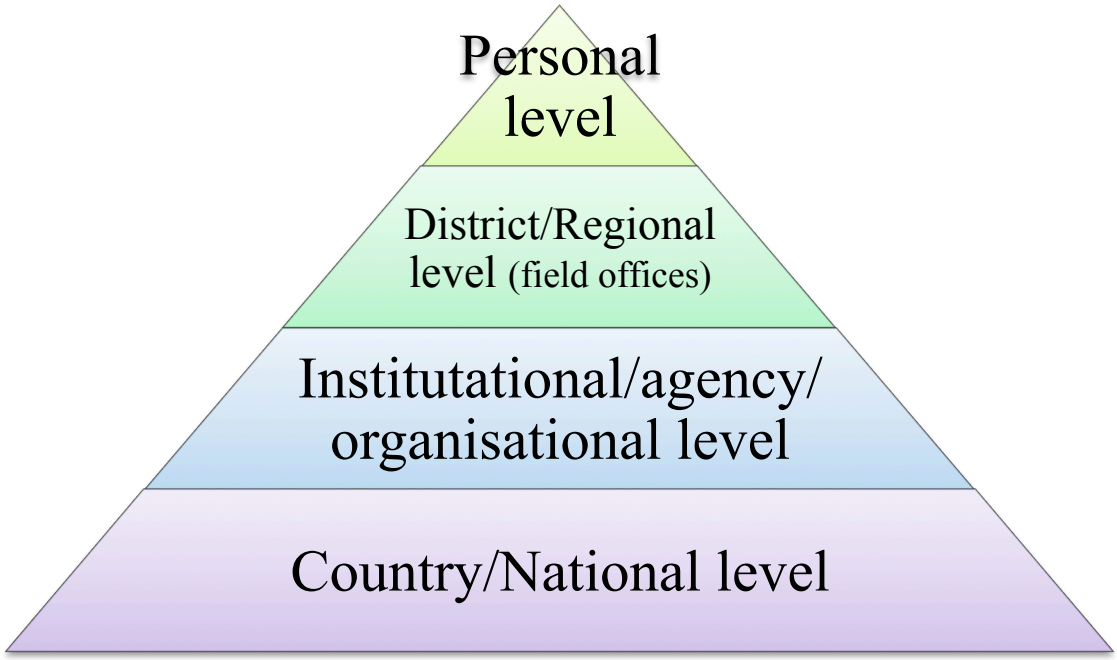
Hannigan (2014) also offers his understanding of why companies vary in their levels of collaboration with the government, which were largely aware of NSA surveillance. He argues that companies would rather present themselves publicly as being neutral

channels of data and political outsiders. However, he claims that the services provided by technology companies have become the 'command-and-control networks of choice for terrorists and criminals' facilitating not only violent extremism and platforms for child sexual exploitation online but also serving as hosts for terrorism and underground criminal activities (Hannigan, 2014). In other words, the ability to dictate cyber trends and their potential to serve as be a driving force in fighting cybercrime indicates that corporations are seen by officials as the 'kings' of the cyber security domain. Correspondingly, governments, policy-makers, prosecutors, law enforcement and intelligence agencies are still lagging behind and have become even more reliant on private stakeholders. This raises the interesting prospect that public-private partnerships may hold the long-term answer to cybercrime.

Finally, it can be argued that governments, law enforcement and private stakeholders may be less relevant to cybercrime as historically *science* has been the game-changer in this area. Moreover, many young people, so-called 'tech geeks', want to work for giant corporations such as Google rather than government agencies. Still, science alone is not a solution in the fight against cyber crime without maintaining trusted relationships between the different stakeholders.

Trust is one of the most important aspects of human interaction; it is also an essential component in any effective corporation or collaborative relationship. Therefore, whether we talk about collaboration on a policy/strategic, legal or operational level, trust is built upon person-to-person level interaction between people with shared interests and commitments over time. Otherwise, trust building among countries could be first established at the national level then further developed on the

organisational, regional and in the end what counts the most on the personal level (see figure 5.2.).



[Figure 5.2.]: *The stages of trust-building*

Trust plays the same vital role in reducing uncertainty when the U.S. and the EU collaborate in the fight against cybercrime. However, there are many potential impediments: to what extent do these two partners really trust each other on a strategic level? Further, how do differences in strategic cyber cultures influence trust-building in the context of data protection and privacy? How have the Snowden revelations affected collaboration on a political, legal and operational level? How have differences in the conception of privacy influenced transatlantic collaboration in the fight against cybercrime?

This chapter will attempt to respond to these questions. While it is acknowledged that policies and laws are constantly developing and changing, nevertheless the following section aims to provide a better picture of the main priorities and approaches adopted by the EU and the U.S. on privacy and cyber crime related issues.

Privacy concerns continue to play vital role in transnational cyber crime investigations. Without doubt, the Internet simultaneously constitutes the largest repository of information and the largest market place on Earth. It also provides the largest and most convenient means of communication, increasingly subsuming other modes. The enormous size of the online market creates huge competition between suppliers who are busy identifying and informing potential consumers. Above all, the personal information of web users is a precious commodity for companies constantly seeking new channels for profit and marketing (Summers *et al*., 2014: 199). Perhaps the greatest illusion perpetrated by the web is that of free services, as Richard Serra famously observed: if the service is free - then 'you are the product' (Serra 1980).

Facebook owns more than 1 billion users' personal information and is a very good example that free membership to online networks can have a huge price: personal information (Vance, 2012). Furthermore, it is an open secret that giant corporations such as Facebook (or Apple) make money through skilfully targeted advertising based on what users share (Creeber, 2008: 104).

According to privacy researcher Christopher Soghoian 'the dirty secret of the Web is that the 'free' content and services that consumers enjoy come with a hidden price: their own private data' (Angwin, 2011). The personal information shared by users for economic and social gain has become a currency of exchange. It is vital to find the right balance between privacy and gain, a balance that currently remains unclear (McStay, 2012: 596).

According to Summers *et al.* (2014), the Internet suffers from an 'endless paradox' which combines openness, privacy and secrecy in seemingly contradictory ways: communication is non-regulated and expressions can be made freely and anonymously, however, the success of the Internet depends on the extent privacy is protected (Summers *et al*., 2014: 200). Finding the right balance between privacy and free expression is vital. If this balance is skewed excessively in one direction this could impact diversity of opinion, free speech and everyday behaviour, together with the way the e-commerce market operates (Summers *et al*., 2014: 200). Inevitably, this touches on many issues beyond the realm of this dissertation including net-neutrality. But it also invites the more relevant question: how is this balance maintained (or not) in the regulatory domestic and supranational regimes of the U.S. and the EU and in their collaboration in tackling cybercrime presumably?

To repeat, this thesis suggests that transatlantic collaboration works well and effectively on the operational level among the law enforcement and intelligence community, however, it is in sharp contrast with the on-going collaboration on the legal and policy level - where differences of legal framework, strategic policies and approaches, lack of capabilities, resources and awareness could often slow down the prosecution of cyber criminals and effective information sharing/gathering between the transatlantic partners.

Therefore, the logic and structure of the chapter will be the following:
First, it will start with the public sphere by exploring the EU-U.S. privacy perceptions that is a vital aspect of strategic cyber culture in the fight against cyber crime. Differences in data protection cultures affect the way strategies and procedures were

developed. Second, the chapter will move on to examine the effect the Snowden revelations had on EU-U.S. collaboration in the fight against cybercrime at the policy and legal levels. It will analyse the strategic dissonance the Snowden revelations made on transatlantic data sharing agreements namely the Safe Harbour, Terrorist Finance Tracking Program (TFTP), PNR and Umbrella Agreements and on the General Data Protection Regulation. Third, the Mazzini case will be used as an analogy to illustrate that Snowden's revelations are also an issue of public policy. It will also talk about the secret sphere where digital intelligence activities are conducted. Fourth, based on the interviews conducted with both EU and U.S. law enforcement officials this chapter suggests that the Snowden disclosures made little or no impact on working relationships - Blackshades will be the case study to elaborate the positive sides of the working relationships between the legal and operational levels. Finally, the chapter will discuss the remaining challenges of collaboration in the public sphere such as the issue with MLATs, data retention, and obstacles to information sharing and cyber security preparedness. Trust building will be examined from an EU angle since developing trust between 28 members is often more challenging than within one country like the U.S.

1. Contesting transatlantic cultures of privacy

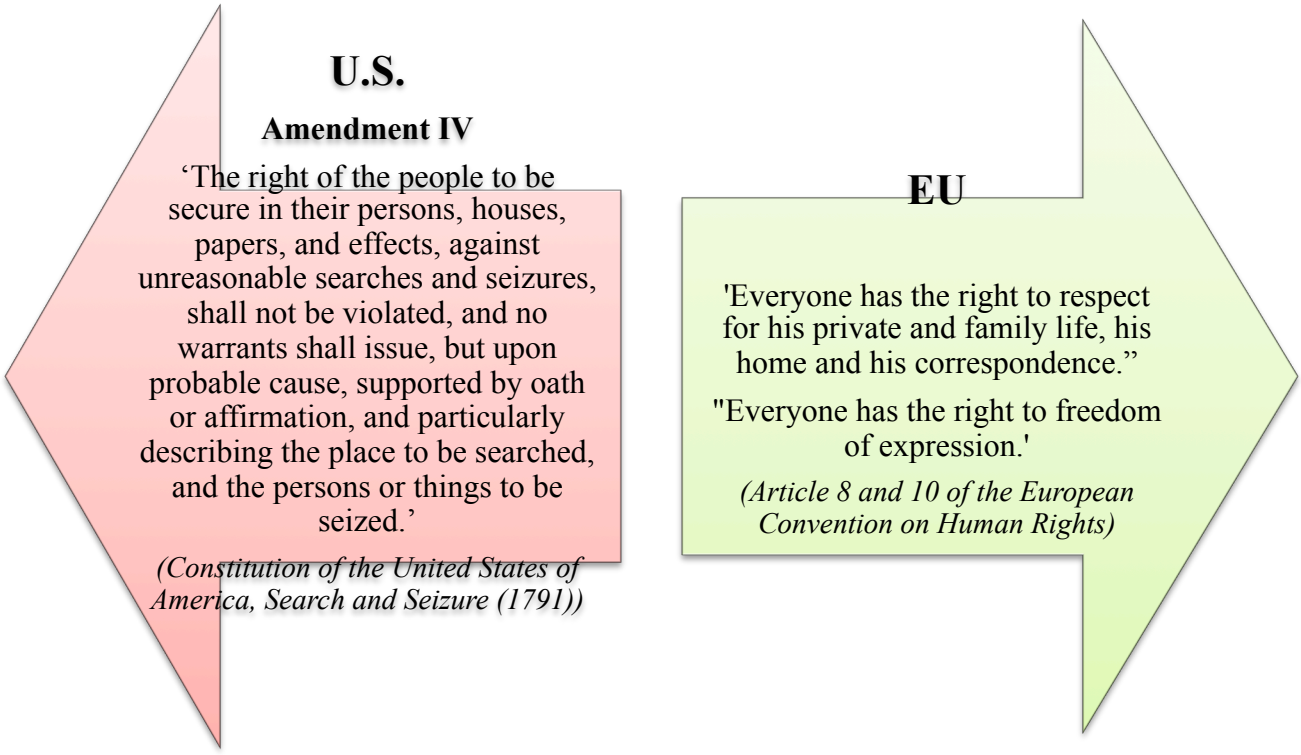
Property bias and the right to freedom of speech have always posed problems for privacy. In 1968 Charles Fried argued that the lack of privacy could pose a danger to 'our very integrity as persons' (Fried, 1968: 477). Since then, many countries, especially in Europe (e.g. Germany), have agreed that privacy is a fundamental right. However, in terms of either political or legal concepts, it remains very difficult to define what we understand by 'online privacy'. As with cybercrime, there is no

internationally accepted definition of privacy. It is often regarded as an existential and elusive term interpreted differently by states and non-state actors according to various contexts and societies.

To illustrate, a cybercrime investigator from the Korean National Police Agency has confirmed that the Chinese government, along with Russia and Brazil, constitutes one of the chief advocates of 'data sovereignty', also referred to as 'Internet sovereignty' (Interview, 2014h). China fears that transnational cooperation in the fight against cybercrime will infringe on data sovereignty and it is paramount for them to protect sensitive national data from foreign surveillance (Polatin-Reuben, 2014: 5). Although they have cultural and linguistic similarities, the Chinese political authorities often block cooperation between South Korea and China. Nonetheless, the 2008 Auction case illustrates that the Chinese government can be cooperative on specifics. In this instance, the personal details of 18 million customers of Auction (Korea's largest online shopping mall) were stolen by an overseas hacker, widely thought to be based in China. The thief then telephoned seeking to blackmail the company (Greenleaf, 2014: 132). How is privacy, data protection viewed and interpreted by the U.S. and the EU?

When conducting field research in Brussels, almost every EU official and law enforcement officer interviewed for this study (e.g. DG Connect, DG Home and Europol) complained that the U.S. has not implemented proper privacy laws and that their approach remains notably different to that of the EU. Conversely, whilst conducting research in Washington, D.C., I often heard U.S. professionals (e.g. a former NSA consultant, DHS officers and former FBI agents) and U.S. Europol

liaison officers from the FBI, USSS and ICE criticise the EU for overregulation of cyber activities. In each case, these professionals had little understanding of the strategic culture that lies behind the different sets of privacy laws on each continent.



[Figure 5.3.]: *Differing views on privacy*

In the EU there is greater emphasis on and a greater expectation of privacy in comparison to the U.S. In other words, whilst Europeans treat the right to privacy as a fundamental right: 'Everyone has the right to respect for his private and family life, his home and his correspondence', as per Article 8 of the European Convention on Human Rights (ECHR), (see figure 5.3.) in the U.S. the right to privacy is often perceived as weak (Whitman, 2004: 1157; Council of Europe, 2010). Nonetheless, private communication encompasses the freedom to communicate as well as the issue of privacy. Therefore, privacy is not only an Article 6 but also an Article 10 issue:

‘Everyone has the right to freedom of expression’ (ECHR). For instance, Germany is a strong advocate of protecting the freedom of speech enshrined in Article 5 of the Basic Law for the Federal Republic of Germany.

> Article 5
> [Freedom of expression, arts and sciences]
> (1) Every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures, and to inform himself without hindrance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship.
> (2) These rights shall find their limits in the provisions of general laws, in provisions for the protection of young persons, and in the right to personal honour.
> (Basic Law for the Federal Republic of Germany)

Although Germany is only a single Member State, it is a vital opinion-former among the EU Member States. It plays a significant role in shaping and influencing EU strategic culture. Moreover, activist human rights lawyers have begun to shift their focus from poorly protected privacy to well-protected freedom of expression.

The emotion that surrounds privacy issues in Europe is comparable to that felt in debates around gun control legislation in the U.S. For instance, many Europeans would be shocked to learn that in the U.S. a merchant has the right to access the full credit history of its customers. However, there is now a plan to introduce chip-enabled credit cards (containing an EMV chip and a magnetic strip) in the U.S. in order to make transactions more secure and to reduce the frequency of credit card fraud that will also impact upon this issue (Interview, 2016b). In contrast, for many Americans there are some aspects of European law that are quite astonishing, such as the practice

of certain European governments that restrict the names parents can give to their children or the strict registration system in place in Germany where everybody must be formally registered by the police whenever they move to a new residence (Whitman, 2004: 1158).

However, while some of the stereotypes are confirmed by detailed research, according to the United States Mission to the EU it is important to debunk the myth that the U.S. does not care enough about privacy compared to the EU (U.S. State Dep., 2012). It is true that while the EU has an overarching Data Protection Framework that is applicable to all Member States across all sectors and is applicable to all types of data, the U.S. has no similar, equivalent, single, all-encompassing core privacy policy that regulates the collection and processing of personal data (Dimov, 2013). Nevertheless, effective privacy law does exist in the U.S. and different approaches to privacy law are adopted on a federal and state level. However, the lack of independent data protection officers and weak power of the Fourth Amendment of the U.S. Constitution - compared to the force of the European Court of Human Rights - demonstrates the fragmentation of the U.S. data protection system (ACLU, 2013).

Whilst on the federal level there is a sectoral approach towards data protection legislation where only specific types of government and industry practices are covered, privacy and consumer protection is dealt with rather more on a state level albeit statutes specific to certain sectors and state-based constitutional rights remain important (Hoofnagle, 2010:1). Some of the more notable federal data protection laws are: the Children's Online Privacy Protection Act (COPPA), which regulates data concerning children and online data in particular, and the Health Insurance Portability

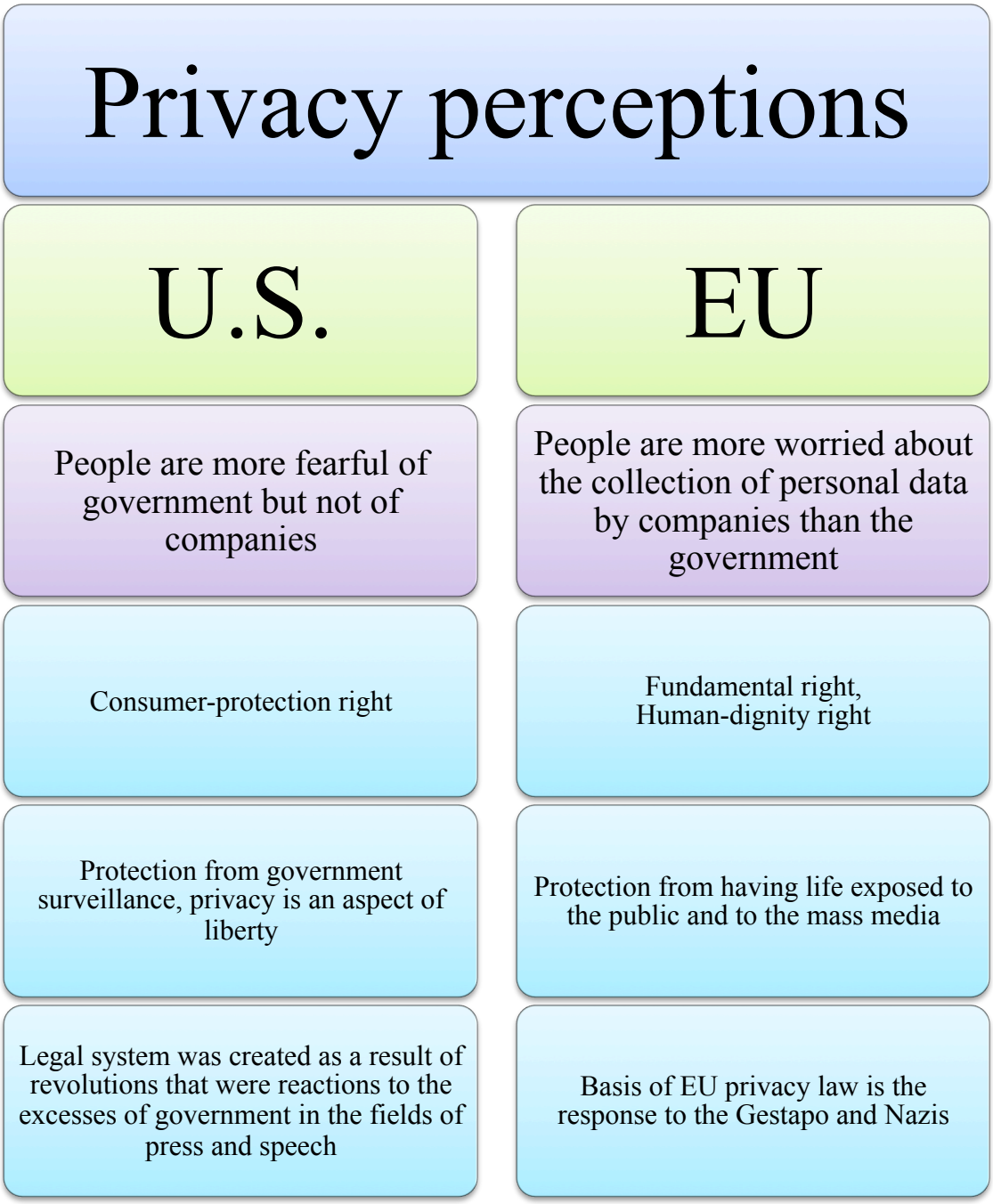
and Accountability Act (HIPAA), concerning sector-specific health-related information (Lee, 2014).

In sum, this chapter suggests that the differences in approaches towards data protection between the EU and the U.S. stem from historical cultural legacies, in other words, from strategic culture. The history of Europe includes a number of periods where certain European countries lived under dictatorships. This historical background helps to explain why data protection is considered a fundamental right by most EU Member States. For instance, the East German police, the Stasi, employed a remarkable 500,000 secret informers among which 10,000 were responsible for listening to citizens' phone calls and transcribing them (Wright, 1998: 10; Margetts, 2012: 24). This historical context of rejected dictatorship also provides an explanation for why the first article of Germany's constitution, written in 1949, places human dignity above all else: 'Die Würde des Menschen ist unantastbar', which means, 'the dignity of human beings is untouchable' (Claassens, 2013: 205).

Conversely, in the U.S., market forces are the driving force behind data protection regulation. Fascinatingly, a former NSA Director suggested that 'Google's policy on privacy plays a much larger and more significant role than the U.S. government's privacy policy' (Interview, 2015w). Nevertheless, it is also important to mention the importance of the state as a countervailing element: the U.S. Patriot Act, which was adopted following the events of 9/11. The Act has markedly increased the power of law enforcement regarding the collection of personal data (Georgetown, 2015).

The concept of privacy is associated with ideas about the self. Many authors have observed that privacy is a curiously existential concept that has little to do with material interests. The paradox is that as global citizens, people want to simultaneously enjoy both local privacy and global shopping; however, privacy is difficult to protect at a global level. In short, you cannot be both global and local – or have your cake and eat it.

Both Post and Whitman suggest an effective method for conceptualising privacy: viewing this either as an aspect of *dignity* or as an aspect of *liberty* (Post, 2001: 2087; Whitman, 2004: 1161). Deploying their perspective, the EU and the U.S. privacy cultures can be generalised as follows: European privacy laws aiming to protect a person's dignity (the individual has a right to control his/her public image, in other words, people can only see what the individual allows them to see), and U.S. privacy laws aiming to protect an individual's liberty (according to the traditional U.S. mentality could be interpreted as freedom from government surveillance/tyranny) (Whitman, 2004: 1161). In other words it relates to the American core focus of freedom (see figure 5.4.).



[Figure 5.4.]: *EU-U.S. privacy perceptions*

Put in a different way, a former NSA Director argued that the U.S. definition of privacy is based on citizenship and is thus a 'process right' protected by the Fourth Amendment of the U.S. Constitution, 'that is the absolute' (Interview, 2015w).

Amendment IV
'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.' (Constitution of the United States of America, Search and Seizure (1791))

Essentially, this means that in the U.S. there is 'absolute protection' for the individual's home whereas the government and the police are kept out of people's private affairs to the greatest possible extent. There is also a strong sense of proportionality or reasonableness in the US framing, even if courts have been slow to uphold this. This is also present in the European case to a large extent, but paradoxically it is felt and implemented more keenly than in the U.S. However, in the public sphere, outside of the home, privacy rules in the U.S. are notably different and there is less of an expectation of privacy. Grounded within the scope of the Fourth Amendment, privacy is 'limited to what an individual seeks to preserve as private, even in an area accessible to the public', for instance, by following the 'plain view rule' privacy cannot be expected to be applied to publicly visible objects (Sottiaux, 2008: 269). To illustrate, any personal information given voluntarily to third parties (e.g. financial records) is not considered to be subject to the expectation of privacy. However, depending on whether they are open to the public, business or commercial properties are sometimes eligible for protection (Clancy, 2009: 334).

In the UK the situation is different again. For example, the Director of the GCHQ, Robert Hannigan, claims that whilst the GCHQ is happy to engage in a public, mature debate about privacy, 'privacy has never been an absolute right and the debate about this should not become a reason for postponing urgent and difficult decisions' (Hannigan, 2014). In addition, Hannigan also suggests that it would be more satisfactory for customers to seek a healthy, balanced relationship between security agencies and technology companies, since many ordinary users (especially those with strong views on ethics) prefer not to see the social media platforms they use promoting child abuse or murder – it is clear that many companies are deliberately not acknowledging its misuse (Hannigan, 2014). All these things are inherently ambiguous: despite the fact that social media could act as a "doorway" for children to become crime victims, it can also play an important role to educate the public and raise awareness about preventing child abuse and neglect (U.S. Dep. of Health, 2016).

Both the U.S. and Member States of the EU continue to try to find the 'golden balance' between privacy and national security, but this is not accepted by all. Some journalists, such as Jacob Appelbaum, the developer of the Tor privacy tool and journalist at *Der Spiegel*, have decided not to return to the U.S. in the wake of Snowden's disclosures (Deutsche Welle, 2013). When conducting field research at the EU Parliament and attending LIBE Committee meetings, it was clear that MEPs considered security to be the U.S.'s sole priority (European Parliament, 2013). Differences in historical and cultural legacies and experiences often provide us with an effective explanation of the different approaches towards data protection and also how they are mis-perceived. However, lurking below, there is still the question of whether some nations are truly pursuing the idea of a golden balance, since there is

often a marked difference between what is going on in the public sphere and what happens in the secret sphere. The interviews indicated that challenges in the public sphere (legal and strategic level) are often stemming from the MLAT process and ECJ's power over data retention that slows down the information that is needed for cybercrime investigations (Van der Meulen *et al*., 2015: 115). Nevertheless, there is an implication here that some of the European public strategies and declarations on data protection and EU cyber security might involve a degree of political posturing and even hypocrisy.

Again, the majority of EU data protections standards are not present or very limited in the U.S. law such as limited inter agency data exchange, an independent oversight, strict proportionality rules, data breaches, exchanges with third parties or correction and deletion rights just to mention a few (Boehm *et al*., 2015: 7). Since the EU approach towards data sharing is driven by protecting fundamental rights and the need to justify every data being shared with third parties and other agencies, in contrast, in the U.S. data exchange between law enforcement agencies and the intelligence community appears to be the norm and not the exception (Boehm *et al*., 2015: 7). The recently introduced U.S. laws such as the FREEDOM Act only helps to enhance the protection of U.S. citizens concerning activities related to intelligence collection. For this reason, all these fundamental differences towards data sharing often hinders and slows down joint cyber crime investigations between the EU and the U.S. at the policy and legal level.

2. Impacts of NSA spying allegations on strategic transatlantic agreements

National security has become a state religion. They say they want to keep us safe, but from whom?
(Thomas Drake, June 2014, der Spiegel)

Following the events of 9/11, the 'Five Eyes', the name given to the intelligence alliance consisting of the U.S., the U.K., Australia, New Zealand and Canada, have greatly extended their signals intelligence capabilities and sharing agreements, placing a greater emphasis on data transmitted over the Internet. Since 2013, former NSA security contractor Edward Snowden has consistently claimed that the Five Eyes is 'a supranational intelligence organisation that does not answer to the known laws of its own countries' (Siebel, 2014). The documents that were leaked on 5 June 2013 by Snowden revealed how members of the Five Eyes have circumvented domestic spying laws by ignoring oversight rules and also by spying on each other and sharing the results. For example, the NSA collects intelligence on UK citizens and then alerts MI5 of any potential threats. There are now vast amounts of raw data in circulation. This raises the question of how an appropriate balance can be established between citizen rights to privacy (or indeed freedom of expression) on social media, Skype and via texts and calls and the need to protect the state from economic threats (e.g. Chinese hackers stealing data on UK companies) and violent threats from non-state actors (e.g. terrorist attacks).

There external threats certainly exist. In essence, today we are witnessing an 'information war' in which organisations (e.g. so-called Islamic State) make great use of archives such as WikiLeaks or the Edward Snowden documents in order to resist

attempts by security services to collect intelligence on their operations. In December 2007, it was revealed that Jonathan Evans, head of the United Kingdom's security service, 'MI5, had sent confidential letters to 300 chief executives and security chiefs at the country's banks, accountant firms and legal firms warning of attacks from Chinese state organisations' (Kiyuna & Conyers, 2015: 177).

Yet in response to allegations of illegal activity by the NSA and its allies, mostly focused on accusations of mass surveillance, a number of political parties in the EU Parliament have asked for existing transatlantic agreements on information sharing to be suspended. The Civil Liberties, Justice and Home Affairs (LIBE) Committee transformed itself into an Inquiry Committee on Electronic Mass Surveillance of EU Citizens in order to get a clearer picture of what has exactly happened and why and to put forward recommendations on how to restore trust in the transatlantic security relationship.

It is clear that on a political/policy level security activities have become less effective since Snowden's revelations emerged in 2013. In particular, data protection has been brought to the fore. For example, former Vice-President of the European Commission (EC) responsible for Justice, Fundamental Rights and Citizenship of the European Union, Vivian Reding, has adopted a challenging stance towards the U.S. and this has constrained how much former EU Commissioner for Home Affairs Cecilia Malmström was able to commit to and be open about collaborating with the U.S. (Interview, 2014f).

The same DG Home Policy Office continued:

The efficiency of the working groups is dependent on the time and commitment of the officials and functionaries working on them, so if you have a top-down view of things then it is bound to affect working procedures and the amount of work to be done. The DG Commission also has its own in-house law and order issues within the EU. External relations and good cooperation is all well and good but they have plenty of other stuff to do. Obviously, cyber security is a global phenomenon and also depends on global relations and the U.S. has been a powerful force. But as a result of aggressively obtaining information from several countries in order to inform their investigations into cyber security, our own national data protection and data retention are also effected (Interview, 2014f).

Three different data flow regulation agreements with the U.S. were re-examined in light of Snowden's revelations: the TFTP Agreement, the EU-U.S. PNR Agreement (these two agreements are related to the fields of justice and home affairs and serve as a tool in the global fight against terrorism and serious crime) and the Safe Harbour Agreement which applies to data transfers in the business domain (EU Parliament, 2014b). On 12 March 2014, the European Parliament adopted a non-binding resolution on the alleged NSA surveillance programme in EU Member States and on its impact on EU citizens' fundamental rights. The adopted text was the result of six months of inquiry by the European Parliament's LIBE Committee. The Committee called for a suspension of the EU-US Terrorist Financing Tracking Programme (TFTP and Safe Harbour Agreements). The suspension was agreed but the amendment calling for the suspension of EU-US negotiations on the Transatlantic Trade and Investment Partnership (TTIP) was rejected. Furthermore, the recommendations made reference to how future breaches of trust can be avoided and recommendations to enhance EU IT security strategy. The proposed action plan includes a 'European Digital Habeas Corpus'. Its goal is to rebuild trust between the two allies while also making sure that strict rules are applied in order to protect the rights of EU citizens (EU Parliament, 2013).

2.1. Safe Harbour Agreement

The original aim of the Safe Harbour Agreement was to address obvious gaps in the U.S. privacy legal framework. However, right from the start Safe Harbour faced a number of political controversies. The Agreement initiated by the EU Commission and the U.S. authorities (i.e. the Department of Commerce, the Federal Trade Commission and the Department of Transportation) equips U.S. companies with acceptable data protection instruments for processing and transferring European citizens' data to the U.S. Among the criticisms made by the European Parliament regarding the Safe Harbour Agreement (Decision 2000/520/EC) was the fragmentation of U.S. protection systems, the lack of a requirement for companies to compensate parties in cases where data is managed improperly and the lack of a right for legal petitions (EU Parliament, 2013). There is now a growing realisation that it is corporations such as IBM and Google who are big players in this area, while states and agencies, even the NSA, are relatively small players. That was one of the main reasons why the EU Parliament voted for the suspension of Safe Harbour.

On 6 October 2015, the European Court of Justice declared that the transatlantic Safe Harbour agreement was invalid (Gibbs, 2015). This judicial act raises the related and broader question of how legal/judicial activism can affect EU strategic culture and its governance of cyber security. For example, Mr Schrems, an Austrian privacy activist filed a claim with the Irish supervisory authority (Data Protection Commissioner) against Facebook following the Snowden revelations. His complaint concerned inadequate U.S. legal protection against the surveillance activities conducted by public authorities (referring to the NSA) when data is received outside of the U.S. (EU Court of Justice, 2015; Walker, 2015). The most important aspect of this claim

was that Facebook is forced to share data with the NSA and thus there are insufficient safeguards to monitor European users' data in this context. This claim was rejected by the Irish Data Protection Authority and was therefore sent before the ECJ. Meanwhile, events have moved on and since the Safe Harbour framework was declared invalid, a new political agreement called the EU-U.S. Privacy Shield has been agreed between the European Commission and the U.S. in February 2016 (EU Commission, 2016).

Nevertheless, partly due to this case, there is the possibility that American companies, such as Facebook, Google, Amazon and Microsoft, will be obliged to physically host the personal data of EU citizens in Europe rather than in the U.S. Furthermore, the claim could lead to bureaucratic chaos wherein American companies with European customers (numbering up to 4,500) are required to follow 20 or more different sets of national data privacy regulations (Cook & Price, 2015).

This episode also demonstrates that ECJ court judgements can be unpredictable and can directly change outcomes and cut across policy. Furthermore, one of the stipulations of the ECJ in its judgement was that whenever the Commission adopts a decision/policy it cannot reduce the powers of national supervisory authorities - but this had in fact occurred in the Safe Harbour case. According to the court findings, the powers of the national supervisory authorities were denied in instances where an individual questioned the compatibility of the Safe Harbour agreement with fundamental rights and the protection of privacy (EU Court of Justice, 2015).

In broader terms, this case reminds us that EU strategic culture is not static but is

always evolving. It also confirms the observations of Lantis regarding how strategic culture changes, insisting that an 'external shock', for instance the ECJ decision to invalidate the Safe Harbour Agreement, can drastically change the policy atmosphere and subsequent decisions (Lantis, 2002: 112).

Certainly a number of the key consequences of the annulment of Safe Harbour are related to the empowerment of EU Member States: (1) EU States now have the power to require U.S. companies to handle EU citizens' data according to their national regulations; (2) Member States can further suspend data transfer to the U.S. and require U.S. companies to host EU data in their country (3) The Irish data regulator can now check to what extent Facebook provided adequate data protection to European users and, in the event that it did not, then there might be the possibility of shutting down data transfer from the EU to the U.S. (Griffin, 2015).

It was in July 2016 when EU-U.S. Privacy Shield – replacing the Safe Harbour Agreement - has been adopted by the Commission and has become fully operational on 1st August 2016. One of the most important aspects of this new framework is the protection of EU citizens' personal data as a fundamental right when transferred to the U.S. (DG Justice, 2016d). Essentially, the framework of Privacy Shield is longer compared to Safe Harbour and includes additional set of principles such as the supervision of sensitive data and the role of data protection authorities. Compared to the Safe Harbour Agreement, Privacy Shield contains commitments from U.S. government and national security officials in writing (Weiss & Archick, 2016: 9-10). However, Germany's data protection authority (DPA) has been vary of this progress and intends to put the legality of the Privacy Shield framework under test in front of

ECJ (Bowman, 2016). The Article 29 Working Party of European data protection authorities (DPAs) also expressed their concern about the lack of provisions to adjust to the new General Data Protection Regulation (GDPR) once it comes into force in 2018 (DG Justice, 2016a).

2.2. TFTP (SWIFT) Agreement

The EU-U.S. TFTP Agreement (also called the SWIFT agreement) plays a vital role in the fight against the financing of terrorism by enabling investigators to discover links across suspected terrorist networks. Coming into force on 1 August 2010, the agreement endeavoured to strike a balance between data protection and privacy and the need to effectively combat terrorism. On 27 November 2013, Commissioner for Home Affairs Cecilia Malmström testified in front of the LIBE Inquiry Committee that after extensive investigations and consultations with the U.S. government no breach of the TFTP Agreement was found:

> The TFTP and PNR agreements regulate the transfer and use of personal data, and provide effective safeguards to protect the fundamental rights of European citizens. We have taken the allegations very seriously of possible US access to Swift financial data outside the scope of the TFTP agreement and, as promised to the European Parliament and the European citizens, we have asked the US to shed full light on this issue. I welcome the reassurances that the US Government has made, including at my meeting at the White House on 18 November, that it has not breached the TFTP Agreement and will continue to respect it fully. But the Commission will continue to carefully monitor the implementation of the EU-US agreements on data transfers in order to uphold EU citizens' rights (Cecilia Malmström on behalf of the European Commission, 2013d).

The same day, the Commission adopted the TFTP Evaluation Report along with an additional report on the joint review of the U.S. Passenger Name Record (PNR) Agreement. Moreover, the Commission also adopted the Communication on a

European Terrorist Finance Tracking System (TFTS); however, no date was scheduled to create such a system. According to Malmström, together with Europol the Commission analysed around 1,000 TFTP reports and found no evidence that the agreement had been breached. During the hearings, Malmström stressed the importance of the TFTP by arguing that TFTP-derived information played a vital role in the investigation of the April 2013 Boston marathon bombings and in uncovering EU-based terrorists training in Syria (EU Parliament, 2013, LIBE Meeting).

In addition, the representatives of Europol (Rob Wainwright, Europol Director) and SWIFT (Blanche Petre, SWIFT Counsel) confirmed in front of the LIBE Committee on 24 September 2013 that the NSA had not violated the TFTP Agreement. Yet the climate of criticism of NSA in the wake of Snowden's revelations was such that, notwithstanding both written statements by the U.S. government and the Commission's own findings that no breach of the TFTP had occurred, the EU Parliament nonetheless voted to suspend the EU-U.S. TFTP Agreement on 12 March 2014 (EU Parliament 2014, LIBE Meeting). In short, the EU Parliament lacked confidence in the inquiry by the EU Commission and suspected a degree of subterfuge. To note, however, the resolution to suspend the SWIFT agreement has been mainly symbolic since it would have require the Commission and the Member States to take action that in reality they are not intend to do (Archick, 2016: 16).

2.3. PNR Agreement

The EU-U.S. Passenger Name Record (PNR) Agreement was determined under Article 24 and Article 38 of the former Treaty of the European Union and entered into force on 1 July 2012 (EU Commission, 2012). The PNR 'are datasets which are

created for every flight passenger by airlines in a computer reservation system' (EU Parliament, 2013, LIBE Working Document). In front of the LIBE Inquiry Committee, Malmström stated that the PNR Agreement had been adhered to and non-U.S. flight data had never been accessed illegally. However, she suggested some possibilities for further progress concerning the effective implementation of the Agreement, for example the improvement of mutuality by allowing 48-hour access to PNR data applicable to all travel data (EU Parliament, 2013, LIBE meeting).

In the joint review of the PNR Agreement it was stated:

> DHS has declared that it shares PNR with the U.S. Intelligence Community if there is a confirmed case with a clear nexus to terrorism and always under the terms of the Agreement. During the review period, DHS made 23 disclosures of PNR data to the U.S. National Security Agency (NSA) on a case-by-case basis in support of counterterrorism cases, consistent with the specific terms of the Agreement (EU Commission, 2013d, Joint Review of the Agreement, SEC (2013) 630 Final).

Nevertheless, there were reservations around the lack of opportunities for challenge. This final report makes clear that there is little opportunity for EU citizens to exercise the right to judicial appeal under U.S. law in cases where their personal data is processed for intelligence purposes, something that the ECHR has identified as important in past surveillance cases (EU Council, 2013). There was an attempt to address this gap under the Umbrella Agreement (data transfer for police and law enforcement purposes), which was voted in as part of the Data Protection Package Reform on 12 March 2014.

In light of the November 2015 Paris attacks, the following December, the Council finally approved an amended text with the EU Parliament on the PNR Agreement in order to prevent, detect and investigate terrorist offences and serious crime more

efficiently (EU Council, 2015b). The new directive explicitly states that air carriers are required to share PNR data with relevant Member State authorities for all flights entering or leaving the EU (EU Council, 2015b). In addition, PNR can be 'handled' only for law enforcement purposes. This further underlines the importance of external shocks, such as the Paris attacks, in generating radical changes in EU security policy, for example, the approval of the EU PNR Directive, which constituted a further substantial change in EU attitudes in this realm.

We might also add that there remain issues of reciprocity. According to a J-CAT member, in the wake of the Paris attacks, the French police had to first ask the FBI to gain access to Twitter and Facebook (Interview, 2015k). Thus, to collaborate with U.S. tech giants, the EU must first go through U.S. law enforcement channels. Reciprocity remains a major issue both at the strategic level of major treaties and also on a work-a-day basis when agencies are collaborating on operations.

2.4. Umbrella Agreement and the Judicial Redress Bill

In September 2015 both EU and U.S. officials made a statement about an agreement they had reached on the protection of data exchanges for transatlantic criminal investigations. Interestingly, the public release of the full text of the agreement happened later (Statewatch, 2015). The Umbrella Agreement will complement existing EU-U.S. and bilateral (U.S.–Member State) agreements in the field of law enforcement. It includes strong data protection rules covering all data exchanged for the purposes of the 'prevention, detection, investigation and prosecution of criminal offences – including obviously terrorism' (Kuschewsky, 2015). The Umbrella Agreement has been blocked primarily due to the fact that European citizens residing

in the U.S. have no right of judicial appeal against U.S. federal agencies when they believe their data has been handled improperly. By contrast, U.S. citizens in Europe already have equivalent data protection rights as EU citizens when it comes to judicial appeal. This constituted an obvious 'one-way street', where U.S. citizens enjoyed more rights than EU citizens. This had to change. Representative Jim Sensenbrenner put forward the Judicial Redress Bill in order to correct the glaring data protection imbalance between the two allies (Volz, 2015).

Accordingly, one positive outcome of the new EU-U.S. personal data exchange for law enforcement purposes (Umbrella Agreement) is that it will provide EU citizens with the same right for legal compensation in the U.S. as their U.S. counterparts whenever their personal data is unlawfully disclosed for law enforcement purposes. This mutual recognition between the two allies can be regarded as a vital step in restoring the trust that was shaken by the NSA snooping scandal and is of symbolic importance.

The Judicial Redress Bill was introduced to the U.S. Congress in March 2015. It will extend the US Privacy Act of 1974 and will grant EU citizens the same rights as U.S. citizens before U.S. courts in instances where their personal data has been violated (Kuschewsky, 2015). According to Representative Jim Sensenbrenner:

'The recent agreement on data sharing between nations is a great step forward for international safety and prosperity … The Judicial Redress Act, however, remains a critical piece in our partnership with the European Union and is critical to ensure continued sharing of law enforcement intelligence. I am optimistic that it will not only be brought before Congress, but will be passed with bipartisan support.' (Sensenbrenner, 2015).

Although the Bill has not yet been adopted, it was publicly announced on 8 September 2015 that negotiations have reached their final phase. The Umbrella Agreement cannot officially come into force until the Judicial Redress Bill has been adopted. The cultural constraint is that EU negotiators insist that EU citizens "enjoy" the same privileges regarding privacy rights and remedies as people in the U.S. These steps are vital in order to narrow the 'cultural gap' between the EU and the U.S. in terms of data protection, once the Umbrella Agreement comes into force it will be important in terms of aligning U.S. views more closer with the EU concept of privacy as a fundamental right and in terms of rebuilding trust concerning EU-U.S. data flows (Thompson & Dossa, 2015). On a positive note, in order to close the transatlantic cultural and privacy gap, in February 2016 President Obama signed the Judicial Redress Bill that was followed by the signing of the Umbrella Agreement in June 2016 (DG Justice, 2016c).

2.5. General Data Protection Regulation

On 12 March 2014, the European Parliament adopted the Commission's data protection reform proposals, on both the *General Data Protection Regulation* and on the *Data Protection Directive in the law enforcement context* (European Commission, 2014). The adoption of the Data Protection Package Reform came at a controversial time for the EU, as Snowden's revelations about the NSA's surveillance activities in June 2013 not only negatively influenced transatlantic security relations but also had a significant impact on the privacy of EU citizens. This wake-up call started a legitimate public debate on the concept of privacy both in the EU and in the U.S. Consequently, the different approaches to privacy and data protection in the EU and

in the U.S. have become more obvious and impacted upon the debate. From a European perspective, data protection is considered as a fundamental right. However, in the U.S. it is mainly regarded as a part of consumer protection (EU Parliament, 2013). The collection of data is already considered to be a data breach in the EU while in the U.S., the collection of bulk data is only considered a data breach if the data is taken out and employed for investigations.

Accordingly, the draft *General Data Protection Regulation* was adopted by the EU Parliament in March 2014 to strengthen and unify data protection for individuals within the EU (EU Parliament, 2014b). In June 2015, the three European legislative bodies, namely the EU Commission, the EU Parliament and the Council of National Justice Ministers entered "Trialogue Discussions" to agree on the final text of the proposed regulation (EU Council, 2015b). In December 2015, an informal agreement was reached at the political/policy level on the new EU GDPR. Despite external challenges such as the Snowden revelations, the reform of the EU-U.S. Safe Harbour agreement and the lack of jurisdiction to regulate the big U.S. tech giants such as Microsoft and Facebook, the regulation entered into force in May 2016 (DG Justice, 2016b).

However, it is likely that these changes will take effect some time from May 2018 (Baker, 2015). Since the European Court of Justice (ECJ) annulled the transatlantic Safe Harbour agreement (this will be discussed later on in this chapter), the GDPR will uphold the "embargo" on transferring the data of non-EU countries that do not meet the "adequate" criteria by the EU (EU Court of Justice, 2015). Furthermore, the reason for the delayed consensus can be explained by the disagreements between the

Parliament and the Council as it takes time for the EU to come up with a single, united voice due to the fragmented approaches and the process of negotiations. The lack of a united voice due to the fragmented EU strategic culture is present in various layers of EU foreign and security policy, therefore, EU cybersecurity policy and data protection regulation are no exception. The difference, however, is that the GDPR is not under a CSDP intergovernmental mandate – so there are more institutional voices and influences (cultures) through consultation/advocacy groups. This is relevant – as the Commission and in particular EP interventions are present at different stages of the policy process (readings).

Regarding sanctions, the GDPR has introduced tough penalties for non-compliance with breached organisations facing fines of up to EUR 100 million or 2% of annual global turnover, whichever is greater. The NIS Directive states that in the case of a data breach, the same sanctions will be applied. Generally, the NIS Directive has been made a bit more "company friendly" in the proposal that has been adopted by the EU Parliament since it states that sanctions are reserved for when organisations intentionally fail to meet the standards required, or are grossly negligent. Nevertheless, the potential fines are very significant.

Moreover, the regulatory policy steps still appear too technical, and *the devil is in the details*. The steps are designed to visibly demonstrate the main priorities of EU data protection policies and to emphasise where they differ from the U.S. approach. These steps also indicate the considerable effort made by the Brussels-led elite to harmonise the different approaches and fragmentations across the 28 EU Member States through regulations.

Today, as we live in a highly interconnected world with a global economy, it is understandable that the rights of data subjects should be respected and protected with appropriate security measures. Without doubt, these regulations on data protection (with severe sanctions and breach notifications) are relatively strict. However, there is still the question of whether the data protection authorities will be provided with sufficient resources particularly in regard to training, which would ensure that compliance with the GDPR is appropriately enforced (Rossi, 2014).

Importantly, the EU considered sanctions against the U.S. over the NSA's surveillance activities. However, although the EU now requires international organisations to keep the data of European citizens in Europe and has proposed the creation of a separate European Internet to shield users from surveillance, the fact that most of the leading tech firms are based in the U.S. cannot be ignored. For this reason, U.S. firms continue to process the data of European citizens whilst hosting that data in U.S. datacentres (Interview, 2015e). This leaves the EU relatively powerless to protect it citizens from the NSA. Interesting though, larger corporations such as Microsoft have opened up processing centres (i.e. in Germany) to comply with this.

3. Lessons Learned: Mazzini Case and the Snowden Revelations

"No man's correspondence is safe. No man's confidence can be deemed secure; the secrets of no family, of no individual, can be guaranteed from reaching the ear of a Cabinet Minister"
(The London Times, 17 June 1844)

The Mazzini case of 1844 is regarded as one of the most significant scandals in the history of state secrecy and the "first modern crisis of public secrecy" (Vincent, 1991: 230). In short, it concerned an Italian radical called Giuseppe Mazzini, who was living in exile in London. Mazzini, the founder of the secret revolutionary society 'Young Italy', was devoted to the unification of Italy. The British Government started to monitor Mazzini at the request of the Austrian Government by systematically opening his letters as they passed through the British post office (Smith, 1970: 191). However, in 1844, Mazzini and his supporters became aware that he had been the victim of what he called "Post-Office espionage" and went to the press with the complaint that the British Government was intercepting his letters (Miller, 2014).

Effectively, this Post-Office espionage scandal had a significant impact. As Bernard Porter (1989) explains, after 1844, "Britain's most continuous and systematic domestic espionage agency for probably two hundred years had ceased operating entirely in the political field" (Porter, 1989: 78). In other words, the practice of issuing warrants for opening secret letters ceased as the result of scandalous public revelations regarding secret security practices.

There is a saying that history repeats itself. The Mazzini case of 1844 is a good analogy to illustrate that Snowden's revelations about the surveillance of digital communication by the NSA are also an issue of public policy that needs to be resolved and that public trust is often fatally disturbed by these sorts of revelations, fundamentally altering cultural perceptions around security agencies. The only difference is that now the battlefield is not the post but the Internet and the method of

interception and data collection is not steaming envelopes open but through the application of surveillance programmes (Miller, 2014).

The 1844 scandal further demonstrates that what society understands of the concept of privacy is not a new issue and has long constituted a matter of public debate. With the emergence of new technologies, we as a society need to readapt and reinterpret what privacy means to us and to what extent we allow surveillance programs conducted both by the government and major companies to influence and monitor our lives. Today, technology is embedded into the fabric of modern society and we have become increasingly dependent on technological devices connected to the Internet. Nevertheless, it is too late to go back to the pre-Internet era as shutting down the Internet, or even restricting its applications, would have disastrous consequences on the critical infrastructures and the world economy as a whole.

However, it can be argued that increased reliance on social networks and the Internet has led to privacy issues. This is accelerating especially in the realm of non-communications data. Many experts are pessimistic about the possibility of privacy. Facebook founder Mark Zuckerberg stated that "the rise of social networking online means that people no longer have an expectation of privacy". Furthermore, according to an interview conducted with a NATO official in May 2014, once you use the Internet and social media, privacy is 'dead' and anything you would like to keep secret is better to be kept in the desk drawer (Johnson, 2010; Interview, 2014c). However, the concept of privacy means something different to each of us. People can be categorised into three groups: first, those who are willing to share personal information about their lives and do so enthusiastically; second, those who prefer not

to share personal data and try to prevent their data from being collected and used; third, those who are in the 'grey zone' who sometimes share information if they want to get something back but prefer to be in control of what personal information is revealed to the public (Miller, 2014).

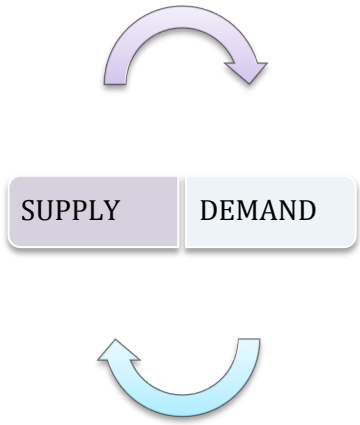
Still, regardless of how hard we try to reinterpret the concept of privacy in the digital age, the main lesson from 1844 (Mazzini scandal) and 2013 (Snowden scandal) is that the collection and processing of personal data cannot be undertaken without the consent and understanding of the public. Therefore, one of the greatest challenges is finding the right way to educate the public about why and how surveillance is carried out in their names and for their security. Without improving society's understanding of the methods of intelligence collection and analysis by providing explanations of what threats they are required to counter, the goals and code of conduct of intelligence work, and the people who do it, the root causes of intelligence scandals cannot be resolved and the arguments over intelligence gathering seems like a never-ending struggle. In this way, the shadows and stigma that surround the work of the intelligence community could be ameliorated by involving various members of the public and explaining the duties and services carried out for common protection more effectively.

Once the public is given sufficient information on surveillance methods and there is a the possibility at least of mutual government–society understanding, a revised interpretation of Hobbes' Social Contract, a 'Digital Social Contract' could come into force. Society needs to understand that surveillance can make the world a safer place, and in order for the government to enforce law and provide security, individuals must

be prepared to give up some privacy. It is impossible for the government to provide 100% security and 100% privacy at the same time. Meanwhile citizens require clear and effective avenues of appeal and redress if they feel things have gone wrong. A balance needs to be established between intelligence practices and protecting the privacy of individuals. However, to agree on the 'red line' cannot be done without the involvement of the public since public consent and understanding is a pre-requisite for the formation of a 'Digital Social Contract'. Furthermore, finding the right balance between national security and online privacy is one of the biggest public policy challenges of our time, not least because the technological background is shifting ever more rapidly.

3.1. Digital intelligence and privacy

Precisely because of our increased dependence on the Internet in everyday life, it is without doubt one of the driving forces of intelligence power. The Internet as an invaluable source of intelligence brings two vital dynamics: first, the unprecedented amount of digital data and information about the public, the government and industry that has been collected and is easily available on the Internet; second, the increasing pressure since 9/11 on the U.S. intelligence community and its allies to gather and analyse information on non-state actors (especially terrorists) (Omand, 2015: 2). The supply–demand dynamic (see Figure 5.5, below) has formed a strong interaction wherein, mixed with technological advances, new opportunities have opened up to allow access to information and radical new avenues to meet national security imperatives.



[Figure 5.5.]: *Supply and Demand*

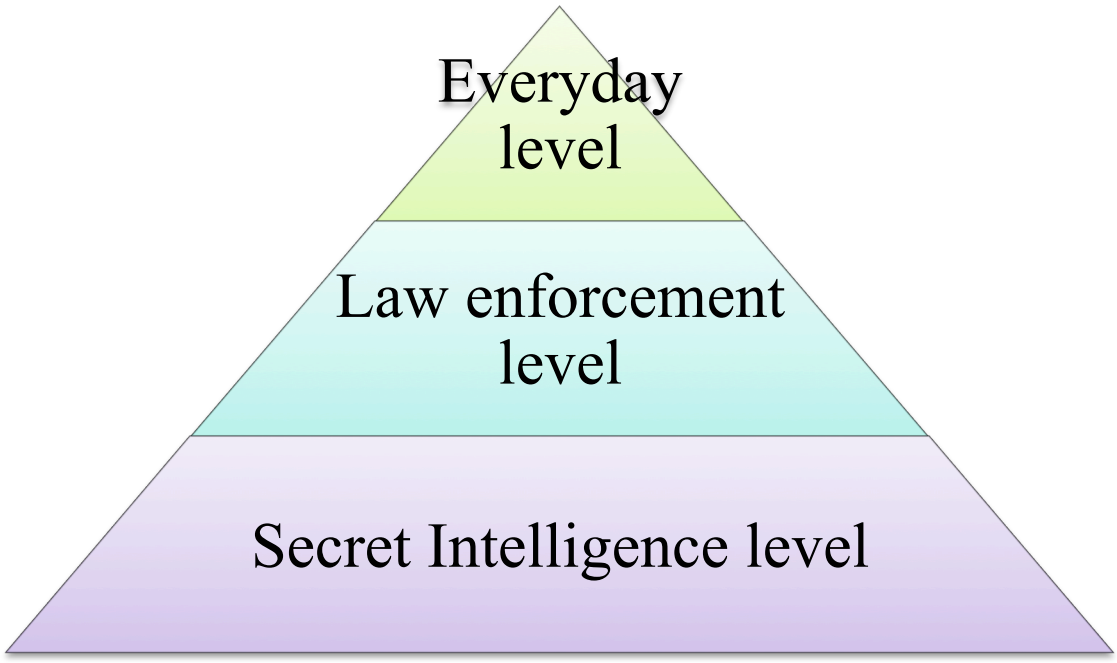
Most of the law enforcement officials (liaison officers) I interviewed at Europol agreed with the proposition that the public needs to be given a clear explanation of how complex legal systems operate. The basis of their argument is that without understanding the nature of intelligence activity, the public may develop a paranoid perspective and think of the intelligence community as being a 'Secret State' whose main role is not to protect citizens against external threats, but to protect the state institutions against their citizens.

This suggests that the nature of digital intelligence activity is made up of three vital factors:

a) What the analysts generate in terms of national demands for intelligence
b) Where the intelligence community goes to meet those demands
c) Considering the ethical and moral consequences of meeting those demands

(Oxford Intelligence Group Seminar, November, 2014).

David Omand proposed a three-layer model (see Figure 5.6, below) to explain the complexity of the different but interconnected layers of intelligence and security activity on the Internet:



[Figure 5.6.]: *Three levels of digital intelligence*

Source: Oxford Intelligence Group (OIG) Seminar Series, 17/11/2014

The **top layer** represents *everyday activities* on the Internet such as banking, trading, sharing, and communication that our society and economy are increasingly dependent on (Omand, 2015: 11). In 2011, the Organisation for Economic Cooperation and Development (OECD) published a set of principles for Internet policymaking to 'help governments to preserve the open and unified Internet that is needed to support economic growth' (OECD, 2011). The Internet economy relies on the free and open flow of information, and the OECD principles help to promote and enable the worldwide delivery of services which are now essential for the smooth running of our everyday lives and the economy (OECD, 2011).

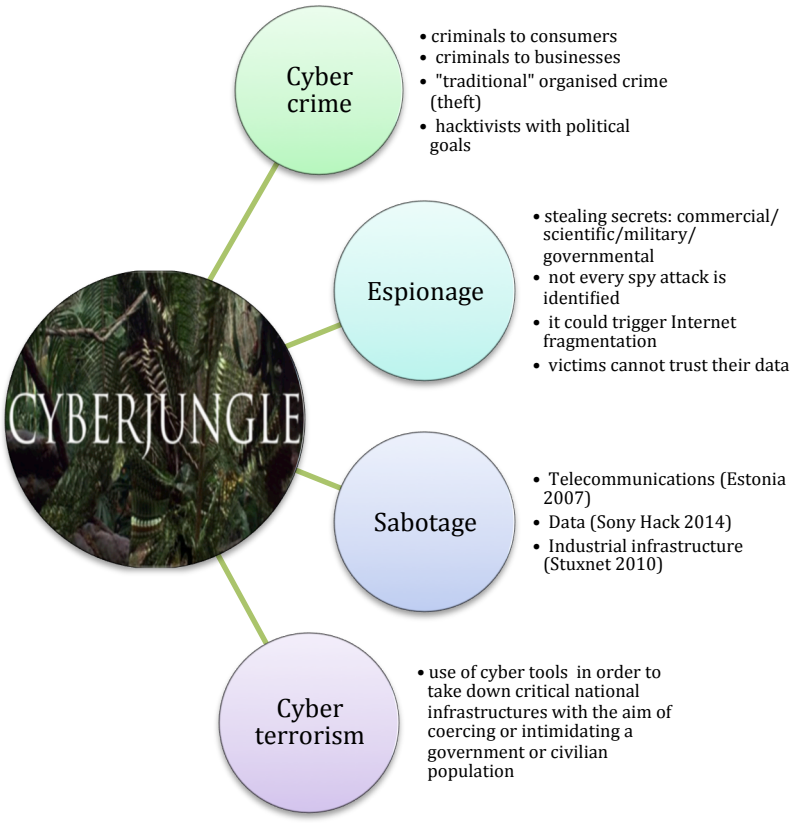
However, the everyday level of Internet use presents not only benefits but also dangers such as cybercrime due to the increased use of malware. Eugene Kaspersky talks about the "ecosystem of the cyber jungle" - drawing our attention to key cyber threats that everyone has to face during the everyday use of Internet:

a) Cyber crime

b) Espionage

c) Sabotage

d) Cyber terrorism



[Figure 5.7.]: *Cyber Jungle*

Source: based on ISCD Information and *Cyber* Security *conference Sept. 2014, E. Kaspersky presentation*

Cybercrime is a greater risk now than ever before due to the unprecedented number of connected people and devices. Financial gain is the main motivation for cyber

criminals and today, they are not only targeting businesses, they are also targeting individual consumers (middle level attacks). There are numerous criminal groups with different intentions, but generally speaking, money is the most significant factor when committing cybercrime. Cyber criminals aiming at consumers target every individual which Kaspersky compares to "catching fish with a net but they do not care of what kind of fish are caught by their net. They just find the best fish and convert it into cash" (Kaspersky, 2014). Attacking Microsoft Windows operating systems is still very high on the targeted agenda and currently, the majority of mobile-based cyber attacks focus on Android[14] devices. iOS users are less vulnerable and according to Kaspersky the reason for this is partially due to the fact that there are fewer Mac OS X Engineers than Windows or Android Engineers (Kaspersky, 2014).

The cyber criminals who target businesses and large enterprises are professional, well organised, and they have extensive resources and highly skilled technical staff with the ability to access the accounts of large corporate banks through fraud, blackmail, or hacking. Some of these groups are also involved in people smuggling. Furthermore, there is a new type of cybercrime emerging that targets ATMs, not to steal account information and passwords but to steal large amounts of money directly from the ATMs (Interview, 2016d). The method the criminals use is to "infect ATMs and bank systems with malware that makes them spit out cash on command" (Smith, 2015).

It is important to highlight the fact that *traditional crimes infiltrate into cyberspace*, which means that criminals develop new types of attacks in order to support traditional crimes (Kaspersky, 2014). Classic crimes such as theft can be easily

[14] Android is a mobile operating system (OS) developed by Google.

carried out in a digital way (for instance, by using malware), which is more convenient than the old-fashioned way of robbing banks. In addition, the criminals do not have to be 'physically present' in the nation that is being targeted.

According to a report by Europol (2013), the cyber attack on the Belgian port of Antwerp demonstrates how organised crime groups use cyber attacks to facilitate the international drug trafficking business (Europol, 2013). The cyber attack on the port is believed to have taken place over a two-year period from June 2011. Hackers based in Belgium were hired by Latin-American drug dealers "to access and breach the computer system of harbour companies and container terminals in order to control the movement and location of the containers" (Europol, 2013; Bateman, 2013). Once uncovered, the Belgian and Dutch authorities confiscated 1,044 kilogrammes of cocaine and 1,099 kilogrammes of heroin, which had been hidden in legitimate cargoes and then shipped in containers from South America (Bateman, 2013).

According to the report, the hackers used two methods: (1) emails were sent to staff members that contained Trojans in the attachment, which allowed the hackers to access data remotely (2) when the initial breach of security was discovered, the hackers broke into offices to fit key-logging devices to the computers so that passwords could be captured (Europol, 2013). As this was the first time such 'modus operandi' had been discovered, it serves as a warning sign to the police and law enforcement authorities that they need to become more tech-savvy and be able to adapt to the new security challenges quicker and more effectively.

Another example of a cyber attack that facilitated theft occurred in Siberia, when mobsters hacked the computer system of a Russian coal mining company, which then enabled the gang to siphon off tonnes of coal and sell it secretly (Kaspersky, 2014).

Criminal activity in cyberspace and the use of cyber attack tools to support traditional crime are not just a European concern. The maritime shipping industry is highly dependent on computer systems and technology, and a report by the U.S. Government Accountability Office (GAO) in June 2014 acknowledges the fact that shipping ports are exposed to cyber security threats since the systems in charge of monitoring the movements of the shipping containers can be hacked for criminal purposes (GAO, June, 2014).

Espionage as well as other forms of intelligence gathering have existed since ancient times. Today, cyber espionage poses a tangible and growing threat to economic security and can have a devastating effect on the social fabric of a nation. As individual, due to our human nature, we always want to know what is 'behind the wall' and arguably the behaviour of nation states is no different.

One of the dangers of conducting cyber espionage is unintentional pollution or proliferation. The possibility that it could spiral out of control and escalate in a domino effect by infecting too many computers, which also carries the risk, that cyber criminals could gain access to espionage technologies and tools. The first consequence is that it would lead cyber criminals to reach out to other platforms such as Linux, Android, Mac, and Windows which would equip them with powerful, professional state-developed tools and the capacity to infect all kinds of systems

(Kaspersky, 2014). The second consequence is that conducting cyber espionage could ruin the trust between nations, which could lead to fragmentation of the Internet, and a significant reduction in investment. Hence, there is a need for international agreements to limit online espionage.

To illustrate this, on the political level, Snowden's disclosures had a negative influence on U.S. foreign policy and damaged the trust between the U.S. and the EU. However, on the working–operational level inhabited by officials – based on interviews conducted in both Washington D.C. and Brussels – it was confirmed that Snowden's revelations did not cause much harm to working relationships. One of the reasons is that the majority of the international intelligence community were already aware of the NSA surveillance programs and shared information with them or even assisted them. For instance, the leaks from a secret BND report in April 2015 suggest that Germany's national intelligence agency (BND) spied on high-level French officials and the EU headquarters on behalf of the NSA (Interview, 2015n). The BND report passed sensitive information, such as the telephone numbers and email and IP addresses it obtained, to the NSA. However, media reports confirmed that the BND has now severely restricted cooperation with the NSA in the wake of the scandal (Connolly, 2015).

Such activity has consequences for general Internet stability and EU-U.S collaboration presumably. Kaspersky argues that "espionage tools are very close to cyber weapons. In the physical world there is a big distance between the button and the bomb, but in cyberspace there are no distances", which suggests that whilst cyber criminal tools such as malware and botnets are designed to steal money and personal

information, cyber weapons are designed to damage and kill (Curtis, 2014). Furthermore, since the line between attack and exploitation by the cyber systems used in espionage and surveillance is blurry it could easily lead to unintentional disruption or major economic loss.

Sabotage in cyberspace can take many forms: (1) attacks against critical information and infrastructure systems (for example, power plants, telecommunications, industrial network, mobile phones, transport, logistics); (2) attacks on data in order to damage and paralyse industries, critical infrastructures, SCADA systems; (3) attacks on industrial infrastructures (for example, Stuxnet or Flame); (4) cyber terrorists using propaganda by posting suicide videos and images online (Jarvis et al., 2015: 27).

The 'dark net' component of the Internet provides a place not only for illegal trading but also via the use of special software products such as Tor which allows users to browse the Web anonymously, the circulation of videos of jihadists' beheadings or images of sexual abuse (Omand, 2015: 12). In addition, the anonymity of the dark net is open to exploitation by criminals and is another area where cyber criminals can have access to increasingly sophisticated malware to carry out cyber attacks.

Cyber terrorism, the misuse of ICT by terrorists, is a growing concern and has become a strategic issue in the prevention of terrorism, especially since the technologies are not only vulnerable to attack but can also be used as a tool to carry out acts of terrorism in the same way that ICTs are used by predatory cyber criminals (Broadhurst, 2006). The objective of cyber terrorism is not monetary gain but to create fear within a target population.

The **second layer**, the middle level, represents the *activities of law enforcement* such as child protection or immigration. Their main task is to "police" the Internet by making sure that the vital services are running accordingly and online activities are operating legally. Law enforcement has a right of authorised access but the liability of Internet service providers (ISPs) is still questionable. The crucial problem is that cybercrimes cannot be committed without the involvement of ISPs. However, should the ISP be held criminally accountable if one of their users commits a crime or should they report the crime once they notice illegal online activity? (Europol, 2014b; Omand, 2015: 13). ISP liability for the activities of its customers is generally based on the extent of knowledge of the customer's activity. If the ISP is unaware of the behaviour of its customer, they are unlikely to be held accountable for that behaviour. Since law enforcement's engagement with ISPs is problematic due to the issues of liability and attribution, they often turn to national intelligence agencies for support. In the UK, for instance, communications data is the most important investigative tool used by the police and also plays a vital role in MI5 operations and all other organised crime cases (OIG, November, 2014).

The **third layer**, the lowest level, represents the *activities of secret intelligence*, which are still related to the policing of the Web. However, law enforcement agencies in many countries are increasingly seeking the support of national intelligence agencies in the detection of crime, to generate leads or gather evidence (Omand, 2015: 14). Although it often happens only after the crime has been committed, digital evidence needs to be provided to the court in order to resolve any doubt. Although the level of collaboration between law enforcement agencies and the intelligence community

varies from country to country, some nations have introduced specific legislation, which authorises the national intelligence community to provide support for law enforcement. National intelligence agencies like GCHQ monitor the Internet partly in order to fulfil the requests from national law enforcement.

Officials claim that one of the documents leaked by Snowden listed some of GCHQ's cyber tools and techniques, the same ones that can be used by criminals against the public, which has 'damaged the capabilities of all intelligence groups to do their job' (Interview, 2015i).

There is still no international law regulating the practice of cyber espionage and indeed no clear definition of what it is. Some nations prefer to "nationalise" their Internet, but the emerging consensus is that this does not improve security and will not advance national security interests, while rendering it more difficult for the commercial world to offer digital services. Nevertheless, as a result of privacy concerns, and also as a result of a desire to control content, some governments want to fragment and 'balkanise' the Internet and create their own intranets to control the flow of information.

3.2. Cybercrime and privacy

According to Porcedda (2011), cybercrime and cybersecurity are attracting increasing national attention, and the protection of privacy and data can be considered a vital element in wider national strategies designed to increase cybersecurity and to prevent certain forms of cybercrime (Porcedda, 2011: 51). Even the European Commission states that EU data protection can play a central role in the security of networks and in

the prevention of online cybercrime (European Commission, 2001). However, Porcedda argues that we should be careful regarding data protection and privacy as the principal solution to the problem, due to the "double-edged nature of cryptography and anonymity". The encryption debate is likely to gather momentum over the next decade. In 2009, President Obama announced his commitment to protect net-neutrality, the principle that all traffic on the internet should be treated equally, by focusing on the free flow of information and privacy (Jensen, 2011). Obama's plan for a free and open Internet is also re-stated in the 2011 *International Strategy for Cyberspace*. The strategy also acknowledges the fact that the provision of good cybersecurity can enhance privacy (Obama, 2011).

Cybercrime knows no borders, and therefore, fighting cybercrime is a complicated multinational issue. Consequently, the establishment of collaboration between the public and private sector in order to prosecute cyber criminals successfully is indispensable for transatlantic cooperation on cyber security and in the fight against cybercrime. However, the true extent of cybercrime is hard to determine, as many crimes go unreported. Although the U.S. has been at the forefront of discussing cyber security issues, the requirement from the government to develop partnerships with the private sector was not confirmed in the U.S. until the establishment of the Comprehensive National Cyber Security Initiative (CNCI) in 2008. In contrast, in Europe, the European Commission already confirmed the public-private partnership initiative in 2000 (European Commission, 2001). However, it is important to mention that the CNCI initiative includes two programmes that could violate privacy: Einstein 2.0 and Einstein 3.0. Pearlman states that while the former reports unauthorised access and malicious content to the US-CERT and is controlled by the DHS, the

Einstein 3.0 programme gives authorisation to both the DHS and NSA to conduct a profound inspection of data entering or leaving governmental networks and inform the appropriate agency instantly (Pearlman, 2010).

Despite these different cultures and approaches, we have seen important instances of transatlantic convergence. The EU–U.S. Joint Statement on 'Enhancing transatlantic cooperation in the area of Justice, Freedom and Security' adopted in Washington in 2009 can be regarded as the first 'transatlantic' document that expresses commitment to fight against transnational cybercrime and other cyber threats against information systems, and also refers to the Council of Europe Convention on Cybercrime (Council of the EU, 2009; Nagyfejeo, 2015: 161). The EU-US Working Group on Cybersecurity and Cybercrime (WGCC) established at the EU–U.S. Summit in Lisbon in November 2010, serves as a framework for future EU-U.S. collaboration to enhance cyber security and cybercrime activities and contributes to countering wider global cyber security threats (EU Commission, 2010a). The Working Group tries to promote a common understanding, a more holistic view of cyber attacks, which often require long forensic analyses in order to track the aggressors. While Member States broadly agree on the important principles, on a technical level, Member States have notably different levels of preparedness (Forum Europe, 2014).

The main goal of this initiative is to develop a shared and common approach to cyber security and cybercrime in collaboration with other regions or countries, which are facing similar issues. The EU–U.S. goals in this regard are:

(1) to formulate global strategies and raise public awareness
(2) to carry out joint and global incident management response capabilities
(3) to foster public–private partnerships

(4) to remove child pornography from the Internet

(5) to advance the Council of Europe Convention on Cyber-crime (2001)

(Nagyfejeo, 2015: 161)

Before the Snowden revelations, this collaboration looked promising on the strategic level. Therefore, in associated efforts to better determine which areas the EU and U.S. could best cooperate in, ENISA and the DHS organised the first joint EU–U.S. cyber exercise, called *Cyber Atlantic 2011* (ENISA, 2011). Furthermore, in April 2013, the EU commissioner for Home Affairs, Cecilia Malmström expounded upon how the EU and the U.S. can further deepen their collaboration on cyber security and cybercrime. She emphasised that cybercrime is a global problem and needs a global response. She focused on three main areas within the overall framework of collaboration that need to be addressed: first, to ensure that law enforcement agencies have access to the best tools and training available; second, acknowledging the fact that the U.S. and the EU take different paths when it comes to the reporting mechanism of cyber attacks, and so, the value of voluntary exchange of information should not be rejected; and, third, the need for children to be protected online through further development of the Global Alliance against Child Sexual Abuse Online (EU Commission, 2013b). This momentum has been paralleled by the EU–U.S. cyber dialogue on foreign policy and the Brussels Summit on 26 March 2014 which also focused on establishing norms of behaviour in cyberspace and the protection of human rights online (EEAS, 2014).

At the EU level, according to Commissioner Malmström, EU bodies such as the ENISA, Europol and Eurojust participate in the four expert sub-groups of the WGCC that work on cyber incident management, public-private partnerships, awareness raising, and cybercrime (Jones, 2011). Furthermore, there are divisions regarding

responsibility and roles: the Home Affairs Commissioner deals with cybercrimes while the Information Society and Media Commissioner deals with issues of cyber security. In comparison, the U.S. seems to be better organised even though there are still intense debates within the White House about how to allocate the cyber security roles among the agencies. The roles are divided between the DoD, the White House, the NSA, the DHS and the FCC, in addition to the agencies and organisations that supervise the WGCC.

4. Operational Cooperation: Cybercrime Case Study - BlackShades

The following section is going to demonstrate the convergence in the U.S. and EU commitments regarding the enhancement of both external and internal cooperation to harmonise the working procedures for law enforcement prosecutions against cyber criminals - despite the fact that law enforcement and judicial activity are only a small part of the transatlantic internal security relationship.

Based on a conversation with an EC3 officer the greatest increase in volume of information exchanged was with the FBI; mostly in the field of cybercrime. This is because of the nature of cybercrime, which acutely stresses the limits of purely bilateral approach but also thanks to Europol's pro-activity and professionalism. With the FBI, Europol has come a long way since it is notoriously difficult to work with them on a multilateral basis. But EC3's exceptional support plus innovative approach, operationally driven with J-CAT, has made the difference. Europol is now the partner of choice for all US authorities in cybercrime. Over all, cybercrime including child

sexual exploitation is now the crime field in which cooperation is the strongest with the US.

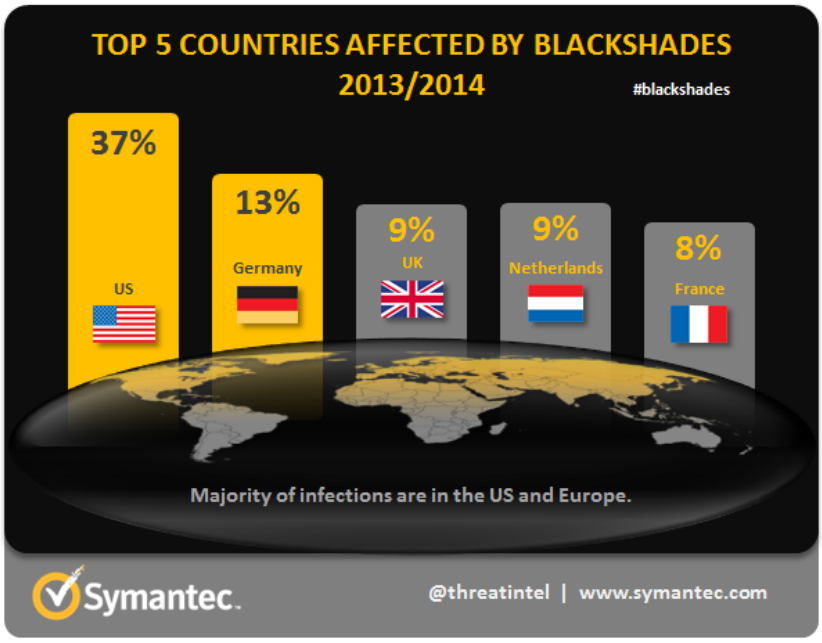
Operation BlackShades is considered to be one of the most successful examples of international cooperation against cybercrime. The operation was coordinated under the "aegis" of Eurojust in partnership with EC3. The following review demonstrates that, in practice, judicial and law enforcement cooperation could work well as long as the working procedures between the operational and legal level are harmonised accordingly.

BlackShades malware, which was developed to allow users to monitor, intrude and remotely control a victim's computer, was originally identified by the FBI through another unrelated investigation (ICSS Conference, February, 2015). The information technology surveillance organisation 'BlackShades' had been selling this malicious software since at least 2010. The software was advertised on underground forums targeting customers who want to spy on their spouses or children in case there is the 'suspicion of cheating' or else if the 'computer is used by the child in an unwanted way' (Kujawa, 2012). Furthermore, BlackShades' flagship product involved a powerful malicious remote access tool (RAT), known as BlackShades NET, which could be used as a tool to deceive the victim in a number of ways, including tricking victims into clicking on malicious links, fake torrent downloads, Java exploits or by hiring others to install the software on the victim's computer (Kujawa, 2012).

When the victim's computer had been successfully infected with the malware, the 'RAT' user was free to 'access and view documents, photographs and other files,

record all of the keystrokes entered and even activate the webcam on the victim's computer - all of which could be done without the victim's knowledge' (Eurojust, 2014). BlackShades also has the capacity to turn the system into a bot that could be advertised at underground bot marketplaces or to launch denial-of-service (DDoS) attacks (Eurojust, 2014).

Furthermore, BlackShades' RAT is an example of a phenomena that operated in a legal grey area since it had been advertised for a "good purpose", however, in reality it was very dangerous. The FBI's investigation has shown that BlackShades' RAT was "purchased by several thousand users in more than 100 countries and used to infect more than half a million computers worldwide" (Dep. of Justice, 2014c).



[Figure 5.8.]: *Countries affected by Blackhades*

Source: Symantec, Top five countries affected by Blackshades activity (2013 – 2014)

Procedures:

The FBI discovered BlackShades' RAT by accident in 2012, and subsequently, acknowledged the need for judicial cooperation at an international level (Dep. of Justice, 2014c: 39). The key to success regarding BlackShades - confirmed during my interview with a cybercrime analyst from Eurojust - is that during the initial investigation, as a first step, each country had their own national targets and had to execute their own investigation of the people who had bought BlackShades with the list being provided by the U.S. (Interview, 2015g). In other words, there were no links between the countries during the investigation. BlackShades is considered an "atypical' case since usually in cross-border cases like this, the Member States communicate with each other when carrying out investigations through coordination meetings. Michéle Coninsx, President of Eurojust, confirmed during her presentation at the International Cyber Security Strategy Congress in 2015 that the corresponding FBI Legal Attaché Offices were in charge of disseminating target packages – including users' identifying information – to foreign law enforcement agencies (ICSS, 2015).

Operation BlackShades is widely considered to be one of the largest global cyber law enforcement operations ever conducted involving judicial and law enforcement authorities in 19 different countries including police agencies and prosecutors as well as EC3, Eurojust and the FBI (Eurojust, 2015b). This is also a unique case where the harmonisation of 'common' operational cultures and working procedures at the law enforcement and judicial levels led to the success of the operation.

Operation Source that managed to "sinkhole" the Beebone botnet can be regarded as another example where international public-private operation was successful (Samani

& Weafer, 2015). The participants in the operation were EC3, J-CAT, the FBI, US Attorney's Office for the Southern District of New York, CCIPS within the US DoJ and in addition private sector stakeholders such as Intel Security, McAfee, Kaspersky Lab, Trend Micro and Shadowserver provided technical assistance, collection of botnet data and threat analysis (FBI, 2015; Shadowserver Foundation, 2015). These steps illustrate that a trusted relationship between the EU and the U.S. is still evolving and the number of successful joint operations will likely to increase in the future. Additionally, Operation Source demonstrates that a strong public-private response with a "healthy" division of labour – law enforcement focusing on operation planning and execution whilst private sector delivers threat intelligence and infrastructure - is necessary to take down a botnet and fight cyber crime effectively (Van der Meulen et al., 2015: 87).

BlackShades' RAT was uncovered accidentally during a cybercrime investigation into credit card crimes by the FBI, termed 'Operation Cardshop'. During this investigation, the FBI arrested the co-creator of BlackShades' RAT Michael Hogue and with the intelligence gathered from him during the follow-up investigation, the U.S. Attorney's Office for the Southern District of New York contacted the Dutch prosecutor who then approached Eurojust (Eurojust, 2015b). This is how the operation started. The next step was a transatlantic division of labour: whilst the U.S. concentrated on taking down the BlackShades' European servers, the EU law enforcement agencies focused on capturing the creators, sellers and customers of the Blackshades' RAT (Eurojust, 2015b).

Representatives from law enforcement agencies of the participating nations attended

three coordination meetings before the subsequent two days of operations:

- the first in November 2013 (NL, BE, DE, FR, RO, USA, Europol/EC3)
- the second in January 2014 (NL, AT, BE, DE, EE, FI, FR, RO, UK, USA, Europol/EC3)
- the third in April 2014 (NL, AT, BE, DE, EE, FI, FR, RO, UK, USA, CA, CL, Europol/EC3) (ICSS, 2015).

These meetings had several beneficial purposes: to resolve legal and investigational challenges, for example, appointing a cybercrime prosecutor in each Member State; real time information exchange on the actions of all the countries involved; discussing how to investigate stored data in the cloud and data retention rules; prosecution possibilities; overcoming the problem of legal differences by providing judicial support for national authorities when in some countries the possession of malware, for instance, is not considered a crime – in such cases the U.S. had to produce a document/report explaining that the use of this malware is only for illegal purposes (Interview, 2015g).

Although the first coordination meeting only involved the U.S and representatives from the EU Member States, other countries were included in the subsequent operation and participated by reaching out to these officials already involved in the operation (Van der Meulen *et al.*, 2015). Eurojust was in charge of overviewing the countries involved and the purpose of the first coordination meeting was to determine which countries had the capacity (both operational and legal) to "take judicial measures against the identified subjects" (Van der Meulen *et al*., 2015). The subsequent coordination meetings focused on aligning the investigation efforts among

the involved states, and information sharing was essential to solve the differences presented by national judicial barriers such as under what conditions a criminal case could be opened (Eurojust, 2015a).

The operation consisted of two stages: first, to dismantle the BlackShades organisation, and second, to stop sales of the software by taking down the Command and Control servers (Eurojust, 2015b). Organising and coordinating the two-day operation presented certain challenges. One of the main difficulties was the timing of the start of the action to ensure it was synchronised between the different time zones. For instance, the law enforcement agencies had to make sure that the house searches were conducted at exactly the same time in each country as the criminals would immediately post information about the searches online to warn other criminals (Interview, 2015g).

The two-day operation started on 13 May 2014. During the operation, "359 houses were searched worldwide, 97 people arrested and over 1,100 data storage devices seized including computers, laptops, mobile phones, routers, external hard-drives and USB memory sticks" (Europol, 2014b). Eurojust played a coordinating role in the operation, providing status reports of the investigations of each participating country and offering legal assistance (Eurojust, 2015b). Meanwhile, EC3 delivered real time analytical support and participated in the follow-up including victim identification and the distribution of technical solutions to prevent the spread of BlackShades RAT (Eurojust, 2015b).

Furthermore, there is some evidence to suggest that Microsoft and PayPal

collaborated with the FBI during the investigation. For instance, the Hacker News website, Wang Wei (2014) mentioned that on various hacker forums, the members had warned each other that the FBI was specifically targeting people who had purchased the BlackShades hacking tool using PayPal, which implies that PayPal had worked in collaboration with the FBI (Wang, 2014). According to the indictment against Kyle Fedorek – one of the customers of Blackshades in the U.S. – the "government obtained a warrant to search the email account 'blackshadessupport@hotmail.com' which then allowed the FBI access to the entire customer database of BlackShades" (Dep. of Justice, 2004).

4.1. Lessons from BlackShades

Several lessons can be learned from the BlackShades case. First, it is a positive example of how cooperation between agents and prosecutors at the international level might be harmonised successfully in order to bring down a cyber criminal organisation. Second, the timing of the start of the action (search, arrest, seizure) in a global operation needs to be synchronised across all time zones (Interview, 2015g). Third, the gathering of intelligence about the victims and the financial losses caused by the malware is important to support criminal procedures, particularly in the U.S. where cases are mostly victim and loss driven (Van der Meulen *et al*., 2015; Eurojust, 2015). Fourth, repressive measures are not enough and need to be combined with preventative action. For example, the UK attempted to deter lower-level purchasers of BlackShades from becoming involved in cybercrime by undertaking preventive activities which included knock and talk visits by law enforcement, warning emails and letters, and this seemed to be a very effective method (Eurojust, 2015b).

Again, from a strategic culture perspective, Blackshades is a good example to illustrate the way various actors in both spheres – public (prosecutor level) and secret (law enforcement level) – can harmonise their work processes and collaborate jointly in a successful manner: Eurojust was responsible to coordinate and provide judicial assistance as well as the delivery of 'status overviews of country-specific investigations' whilst EC3 helped in the provision of analytical support, identification of victims and the advancement of technical solutions (Eurojust, 2015b; Van der Meulen *et al*., 2015).

5. Remaining challenges in the public sphere

This thesis suggests the U.S. and the EU have different perspectives on the most important goals for transatlantic cooperation regarding cyber security. At the policy level, the question of how to find a healthy balance between security and freedom (e.g. the right to privacy) often arises between the two sides of the Atlantic (Bendiek, 2014). However, this also leads to the question of whether it is feasible to have 100% security and 100% privacy at the same time online since both freedom and security are competing values and whether, if there is an undue focus on one – it will 'override' the other. In short, to what extent is this a zero sum game?

Bendiek (2014) argues that the U.S. approach to cyber security is driven by the "military logic of deterrence" which involves maintaining an offensive capacity to protect its traditional infrastructure. In contrast, the EU considers cyber security more as a police matter and tries to prevent the exploitation of fragmented

infrastructure by strengthening resilience among the Member States and their resistance to attack and fraud (Bendiek, 2014: 2). The different approaches of the U.S. and the EU to cyber security could be regarded as a reflection of the federal structures that are strongest on each continent. However, this research suggests we should avoid generalising about the U.S. and EU responses to tackling cyber threats or seeking to cast up one overarching single approach. The different approaches at the horizontal level (policy, legal, operational) or organisational/agency level instead suggest a fragmentation of responses, thereby generating many cyber security cultures and views depending on which angle we are looking from. Again, it is also important to note the gap in working procedures when dealing with cybercrime at the legal and operational level. The widely different views and approaches here about how to best handle cyber investigations were also confirmed during the interviews conducted for this research.

Furthermore, the different organisational cultures of state and sub-state entities that are allocated to different tasks within the cyber security domain suggest divergent transatlantic attitudes regarding the issue of information sharing, privacy and civil liberties.

Notwithstanding this, some broad observations can be made. From the perspective of the Department of Defence, while the U.S. tries to maintain its position as the dominant power in the international system, U.S. cyberspace policy continues to be driven by national security issues, with a focus on deterrence. However, for the EU, data protection will remain the central issue as the EU has adopted a police approach to cyber security and their main goal is to strengthen resistance and

resilience capacities to combat cybercrime. In addition, the EU continues to broaden ICT protection to all parts of the digital economy including Internet platforms and social media (Interview, 2014i). By contrast, the U.S. focuses more on the protection of traditional infrastructure and, remarkably, does not include the digital economy when it comes to ICT protection (Interview, 2014i). It is also important to note that the EU's aim of achieving "unitary, binding regulation is shared by the Obama administration and the U.S. Senate but not by the majority of the House" (Bendiek, 2014: 20).

Furthermore, different legal systems have been developed as a result of the different strategic cultures. Comparing the legal systems in the U.S. and in the EU (including the different national legal systems), we can see that specific circumstances and different geostrategic experiences and positions have pushed them to develop rather different legal environments. A critical aspect of this is the different privacy needs of these stakeholders and the need for development and collaboration in accordance with cultural norms and national legislation in the two regions where privacy enjoys different philosophical and legal definitions.

5.1. Jurisdictional problems in investigations

Although the BlackShades case is deemed to be one of the most successful cybercrime cases ever conducted, and while there is continuous improvement in transatlantic collaboration at the operational and intelligence level, challenges remain and there are still grey areas especially at the legal level.

For instance, a grey area that DG Home has been working on is Internet Protocol version 6 (IPv6). Quite simply, there has been an upgrade from IPv4 to IPv6, which is the most recent version of the Internet Protocol[15] (IP). The FBI has been cooperating with EC3 to ensure that this development in Internet Protocol does not make it too easy for cyber criminals to abuse the system (Interview, 2014f). Since the late 1980s, due to the dramatic growth of the Internet, there has been the problem of IPv4 address exhaustion. To address the anticipated shortage of IP addresses using IPv4's 32-bit address space, the Internet Engineering Task Force created IPv6 to replace IPv4 (Raicu and Zeadally, 2003).

The paradox is that whilst IPv6 will enable users to have a whole set of different ports connected to one IP address, which is helpful in terms of providing more Internet domains, at the same time, it also makes it possible for one Internet domain to be used by 30 or 40 different people or identities. Therefore, from a security perspective, the new protocol version makes it harder to identify, prosecute and gather evidence about a criminal using an IP address (Shinder and Cross, 2008: 52). Troels Oerting, former head of EC3, confirmed that since there are tens of thousands of IP addresses behind one Internet domain, law enforcement must rely on the Internet Corporation for Assigned Names and Numbers[16] (ICANN) to sort out what data belongs to which people (Cyber Intelligence Europe, 2014). Therefore, it can be assumed that ICANN increasingly wields the most power when it comes to the question of who is in charge of the Internet.

[15] IP is the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.
[16] ICANN is the non-governmental organization tasked with assigning IP addresses to machines and Web properties.

5.2. Mutual Legal Assistance Treaties

Digital evidence gathering is one of the most crucial and challenging parts of international cybercrime investigations especially when electronic communications and other data records need to be obtained from countries that are outside the domestic jurisdictional framework. Digital evidence gathering at the legal and strategic level - compared to intelligence exchange at the operational level - is often very time consuming, and cumbersome as there is no free movement of evidence exchange. The 2002 Supplemental Agreement between Europol and the U.S. on the exchange of personal data allows the exchange of operational data between Europol and the U.S. which is an important measure aimed at enhancing the safety and security of EU and U.S. citizens (Interview, 2015m). This legal agreement breaks down the barriers to exchange information effectively at the operational level. However, when it comes to strategic partners, Europol cannot provide personal/operational data due to the absence of a relevant legal agreement (Interview, 2015m).

According to the U.S. DoJ, MLAT requests are "a formal way in which countries request assistance in obtaining evidence located in a foreign country for criminal investigations and proceedings located in another country" (Dep. of Justice, 2015b). The types of assistance that can be provided through MLATs include: service of documents, search and seizure, sharing of telephone intercept material, gathering of evidence from witnesses. However, the MLAT request process is very time consuming as it requires an administrative legal process in each country (Van der Meulen et al., 2015). Kent (2014) provides a detailed overview of the legal processes involved in obtaining data from abroad. She explains that in order to obtain communications data

from the U.S., investigators in the UK and other countries have three options: (1) through a formal MLA request (2) using ad hoc arrangements which means that companies/providers could decide whether to share information on a voluntary basis to non-U.S. law enforcement requesters or (3) through joint investigations with the U.S. especially if there is a "clear U.S. dimension to the crime" (Kent, 2014: 5).

However, the process of requesting an MLA can be 'delayed further if national legislation requires that MLAs are sent via traditional postal services or if the government does not provide an online submission form' (Kent, 2014). In the UK, an MLA request can take between eight and 13 months, while in the U.S. the average time is around 10 months (Kent, 2014; White House, 2013a: 227). Furthermore, in the U.S., the Electronic Communications Privacy Act puts legal limitations on under what circumstances U.S. providers are authorised to share the contents of emails with non-U.S. countries - which is usually the requirement to establish probable cause that a crime has been committed (Interview, 2015f).

MLAT Procedures: Every country has a central authority that deals with these official legal requests. Kent (2014) explains that when a U.S.-UK MLAT is requested, the first step in the process is that the Crown Prosecution Service forwards a letter of request to the UK's Central Authority in the Home Office. The Central Authority checks whether the request adheres to the Treaty regulations and then forwards it to the U.S. Central Authority, which is the Office of International Affairs (OIA) at the DoJ in Washington, D.C. (Kent, 2014: 5). The OIA serves as the U.S. Central Authority with respect to all requests for information and evidence received from and made to foreign authorities under MLATs regarding assistance in criminal matters

(Interview, 2016a). Before forwarding the request to the relevant U.S. Attorney's office in the District where the provider is located, the OIA will review the MLAT to ensure it complies with the Treaty and will then translate the request into a U.S. legal document which can be either an administrative or legal subpoena or a court order which is forwarded to the recipient company. The location of the provider is often Silicon Valley, which is in the Northern District of California (Kent, 2014: 5). Once the company has given their response to the legal order, it is forwarded back through the U.S. law enforcement office where the data is processed and interpreted to meet the requirements of the foreign investigation (Kent, 2014: 5). After that, the response is returned to the original Crown Prosecutor (in the case of the UK) and the law enforcement requester via both Central Authorities for verification (Kent, 2014: 5).

Those working within the system find the MLAT request process slow, and ineffective, and these problems were repeatedly confirmed by the interviewees (DoJ prosecutors, FBI officers and Eurojust officers) who pointed out to the need to reform the way information flows between law enforcement agencies and governments. Furthermore, a report from the Global Network Initiative 2015 also highlighted the inefficiency of the MLAT process which can take months or even years in some cases (Woods, 2015: 3). Therefore, it is not surprising that the cyber criminals benefit from the slow digital evidence gathering of transnational cooperation at the legal level. However, law enforcement agencies have taken positive steps to make transborder cooperation more effective such as the creation of the Joint Cybercrime Action Taskforce (J-CAT) under the aegis of Europol's EC3, to coordinate international investigations, to assist the exchange of strategic information, to process MLAT requests and to provide face-to-face platforms (Van der Meulen et al., 2015: 93).

As an alternative to MLATs, two or more EU Member States could set up Joint investigation Teams (JITs) to share investigative information. According to an USSS Special Agent, federal law enforcement agencies can only participate in JITs as associate members due to the current legal constraints imposed by the U.S. DoJ, – this includes foreign partners (Interview, 2016c). The Assistant Attorney General made the decision that U.S. federal agencies cannot fully participate in international JITs but currently they are working to change this procedure. However, in the U.S., JITs are common between the ICE, FBI and USSS (Interview, 2016c). The USSS Special Agent also suggested that the reason for not participating in international JITs could be attributed to the various digital evidence-gathering procedures that exist among the EU Member States which are different from the U.S. Furthermore, a JIT refers only to one investigation and is handled by only one court – usually a non-U.S. court, which means that U.S. law cannot be applied.

5.3. Data protection and retention

Data protection and retention plays a vital role in the EU's collaboration with the U.S. on cyber security issues but often slows down investigations on the legal and strategic levels due to divergent views and different legal procedures in data protection; in short due to the EU greater culture of caution in this realm.

While the EU treats the issues of data protection and privacy as fundamental rights, data protection still enjoys a more questionable status in the U.S. and the regulation is quite fragmented (White House, 2009: 20). As a result, in June 2013, further disputes

over EU-U.S. data retention policies flared up again as a result of the NSA spying revelations leaked by Edward Snowden.

The privacy risks and vulnerabilities that appeared with the introduction of computers however went ignored from the beginning:

Computer pioneer and RAND researcher Willis H. Ware demonstrated insights ahead of his time and is widely remembered for his prediction of how computers would come affect our lives: ‘The computer will touch men everywhere and in every way, almost on a minute-to-minute basis’ (Ware, 1966). At the Spring Joint Computer Conference in Atlantic City in 1967, Ware cautioned against the risks involved in storing sensitive data in a multiprogramming system (Warner, 2012: 783): ‘By their nature, computer systems bring together a series of vulnerabilities. There are human vulnerabilities throughout; individual acts can accidentally or deliberately jeopardize the system's information protection capabilities’ (Ware, 1967: 11). The infeasibility of attaining security in a multiprogramming system was concurred by Bernard Peters, the director of the NSA’s RYE system, and a panellist at the conference (Peters, 1967: 283-286; Warner, 2012). During the 1970s, Ware foresaw that there would be ‘no engineering solution’ to the COMPUSEC problem, arguing that it would be highly unwise to store classified information in an open system comprised of ambiguous users connected by unprotected communications (Ware, 1970; Warner, 2012). Essentially, the argument here is that hardware is less important in computer security than up-to-date housekeeping (Warner, 2012: 785).

Criminal acts such as computer data theft and espionage were already a concern in the early 1960s, as users identified ways to compromise data that computers were sharing. According to U.S. Cyber Command historian Michael Warner, the first case of computer espionage was likely to have occurred in 1968 within IBM's German subsidiary, when the West Germany police force captured an East German spy (Warner, 2012: 784; Healey, 2013: 29). Policy documents were created by the DoD, together with intelligence communities, as a consequence. These were the 1979 *DoD 5200.28-M Directive* and its *ADP Security Manual,* which introduced the first COMPUSEC standards designed to 'prevent accidental or malicious intentional violations of system security and provide historical records of such transactions' (Ware, 1987: 6; Herrmann, 2001: 39; DoD, 1979). The next major step in this area was the release of the *CSC-STD-001-83, the Trusted Computer System Evaluation Criteria* (TCSEC) (also known as the *Orange Book*), which was presented by the U.S. DoD in 1983 (Herrmann, 2001). The *Orange Book* was a first draft effort to provide initial guidelines in order to tackle the COMPUSEC problem by rating the strengths of computer systems that 'implement security controls and enforce a security policy' (Ware, 1987: 12).

The above examples illustrate how the strategic-military mind-set of the U.S. has developed since the early 1960s, providing deeper insight into the trajectory on which the U.S. has shifted, and helping to understand why the U.S. perceives cyberspace as a battleground. Reflecting for a moment on the paper that Ware presented almost five decades ago, it is clear that his concerns about information privacy have now become a reality that must be dealt with. The rapidly changing nature of cyber security still presents a challenging problem, and 'the prevalence

of international corporations makes it difficult to govern anything in this realm on a singular basis' (Nagyfejeo, 2015: 148). The effective way in which the EU and U.S. have managed to collaborate in coordinating private partnerships represents one of the most successful recent developments in this area. However, one of the critical aspects of governance is that the different stakeholders (e.g. the civil population, private and public sector, and those in academia) need to assess their own privacy needs and, therefore, there is a need to ensure each party is able to achieve effective collaboration and development in accordance with the relevant cultural norms and national legislation.

Europol and privacy

On 19 March 2014, at the LIBE Committee meeting on 'EU Internal Security Strategy and enhancing police cooperation' Rob Wainwright, the Director of Europol, welcomed the adoption by the European Parliament of the Data Protection Package but expressed three major concerns regarding data protection and Europol (EU Parliament, 2014a). Firstly, law enforcement agencies need to restore the public trust they lost after Snowden's disclosures on government surveillance. He argued that police cooperation needs the support of the public because community consent is an important precondition for successful police collaboration. Secondly, according to Wainwright, within the adopted Data Protection Package, the voice of police community could have been made clearer by highlighting that Europol is proud to have one of the most robust data protection frameworks in the world of law enforcement and respects the right to privacy and civil liberties (EU Parliament, 2014).

He expanded on this second point by explaining that common standards of data protection and privacy should be applied differently in the realm of police and law enforcement as against public administration. To explain this principle, Wainwright mentioned that when Europol collaborates with a national police force to arrest a suspected criminal, it is essential to apply the highest data protection standards (different from general data protection principles) so the suspected criminal or mafia does not notice that the police are in pursuit. Therefore, fundamental principles do not apply in the same way in the law enforcement world.

Thirdly, Wainwright warned of the danger of criminals migrating online. Our increased connectivity has created new opportunities for criminals bringing increased risk of theft, fraud, and abuse. He mentioned that attacks online mostly come from private actors and regrets the fact that there is no current regulation that would allow Europol to receive information from private parties to assist investigations (EU Parliament 2014, LIBE meeting).

Despite the fact that EC3 was established in February 2013 and aims to become the focal point in the EU's fight against cybercrime, Europol still lags behind. Consequently, the sheer gap in terms of power capability between police and the private sector raises important issues about the governance of the Internet where police capability online is a significant question for the legislators. An additional problem is that financial institutions tend not to report to the police if they have become the victim of fraud because they are afraid of damaging their reputation. Therefore, there is still long way to go in order to make sure that there is compliance even with the current conventions.

After these revelations, the European Commission expressed the need to restore trust in the way in which companies and governments process data.

Arguably, the U.S. government is no longer the dominant actor within the 5th warfare domain – cyberspace. The 'methods of convergence' are also present within the private sector not just in the state-dominated public sector (Interview, 2015w). As a consequence of the leaks exposed by Snowden, giant companies such as Google and Apple came up with the idea of selling devices that are encrypted by default. By storing the encryption keys on the device, without the passcode, no one – not law enforcement or even Google or Apple – can break the encryption. One of the reasons for these actions is to sell these products in Europe, or to European partners. In this way, U.S. giant tech companies are hoping to regain the trust that has been shaken following the NSA leaks, however, 'the White House and the FBI are not satisfied about these actions and would like to make encryption illegal' (Interview, 2015w). Therefore, there is still the question of to what extent these giant tech companies will manage to re-establish the trust in Europe and beyond.

National data retention times can be regarded as a further serious challenge when attempts are made to obtain information from a number of countries to keep investigators informed. Moreover, law enforcement agencies need to collect digital trace evidence (e.g. IP addresses) to start an investigation (Interview, 2015h). However, if the data has not been preserved by the national authorities, then digital trace evidence cannot be gathered which makes it difficult for investigators and

prosecutors to begin an investigation and compile a legal case against a cyber criminal (Van der Meulen et al., 2015: 93).

In other words, current data retention laws are inadequate for law enforcement. The majority of intelligence and evidence for cyber investigations comes from the private industry. According to a Europol officer 'With no data retention, there can be no attribution and therefore no prosecutions. In this context a new EU Directive on data retention, following the European Court of Justice's annulment of the Safe Harbour Agreement is urgently required' (Interview, 2015h).[17] From a law enforcement perspective, short data retention times can further add to the weakness and fragmentation of transnational collaboration and efforts in the fight against cyber crime. One of the most common complaints from law enforcement officials is that data is often stored only for six months and there are also countries where there are no data stored at all and as a result it is almost impossible to launch investigations (Interview, 2015h).

Despite the presence of common operational cultures at the secret sphere that contributes a lot to the success of cyber crime investigations, if there is fragmentation at the public sphere around issues such as data retention and privacy it could slow down investigations and hamper transnational law enforcement efforts to understand how cybercriminal networks run and develop over time.

Therefore, a consistent and harmonised approach towards data retention, law enforcement procedures whilst ensuring strong alignment towards data protection and

[17] It is important to note that the interview was conducted before the Umbrella Agreement was signed in June 2016.

privacy would be a vital step forward in order to make fast and accurate decisions about the nature of cyber crime activity and what effective methods need to be applied during the cyber crime investigation to remedy the problem.

5.4. Trust building and information sharing

It is important to emphasise that over the last 20 years, there have been significant developments in EU-U.S. information sharing techniques to facilitate the common fight against transnational crime and terrorism. According to Occhipinti (2013), both the EU and the U.S went through different stages of *intelligence reform* that occurred largely in response to new security threats and perceived intelligence mission failures (e.g. the 9/11 attacks, Madrid and London bombings, 2004/2005) (Occhipinti, 2013: 143).

Although the U.S. and the EU both recognise the importance of sharing information, one of the major challenges to the information sharing process relates to the notably different institutional structures and contexts that they have managed to develop throughout history. Mutual information sharing is also a question of trust among players that share similar values, cultures and philosophies, which can be established either at a country/institutional/regional level but most importantly at a personal level. Lack of trust at any of these levels represents the final obstacle to the 'willingness to share' criminal intelligence and security data. The U.S. liaison officers at Europol explained that they are careful when sharing operational data with other non-U.S. law enforcement entities because if they share the data through multilateral channels they cannot be sure where the information will end up even though the EU is considered as

a valuable partner. Therefore, they prioritise the bilateral channels that they have already established and seek to develop strong person-to-person relationships.

The EU Member States struggle to overcome their political, legal, cultural and linguistic differences that have shaped the existing European law and bilateral relations in order to make information exchange more efficient in an international setting. By contrast, in the U.S., the flow of information is situated in a domestic environment both horizontally within the U.S. government between both law enforcement agencies and the intelligence community, and vertically with State, local, and private sector partners (Occhipinti, 2013: 154). Furthermore, another problem is that the EU does not have a single, united voice when it comes to responses to security threats due to the various divisions that are present among the agencies responsible for border management, security, intelligence and law enforcement compared to the hierarchical organisation of the U.S. intelligence community. While the sixteen members of the US intelligence "community" might be considered divergent, the club of European national intelligence and security agencies extends to over a hundred entities.

Snowden's revelations about the NSA's mass surveillance activities rocked the transatlantic relationship, and therefore, we can assume that continued transatlantic intelligence cooperation has required "clarifications" from the U.S. to explain why the U.S. spied on her European 'friends'. Although President Obama claimed in his speech *on Reforms to National Security Agency Programs* at the Justice Department that 'We do not collect intelligence to provide a competitive advantage to U.S. companies or U.S. commercial sectors', many still privately wonder whether

economic espionage was the motive for NSA spying which is not justified by national security imperatives (Department of Justice, 2014a). For instance, it is apparent that there are no terrorists within EU institutions that could pose a threat to the national security of the U.S. but eavesdropping on these organisations would give the US the possibility to extract valuable information about high profile economic decisions or trade negotiations. Furthermore, an independent analysis of 225 terrorism cases conducted in the U.S. in 2014 came to the conclusion that the NSA's bulk collection of phone records 'has had no discernible impact on preventing acts of terrorism' (Nakashima, 2014).

Obstacles to effective information sharing

Officials often suggest that the reason why certain Member States prefer not to cooperate with each other can be explained by five convergent factors, which, while different, often interact. These can be summarised as differences in capabilities, resilience, capacities, confidence and interests (Interview, 2014j). It has been argued that this is not necessarily linked narrowly to the cyber field as such but to an overall experience with certain Member States when it comes to the question of national security.

In terms of what we might call national security texture, two groups can be distinguished:

1) Bilateral alliances between specific Member States that are at the forefront and are very well advanced in their own strategies and policies such as the UK, Germany, France, Netherlands, and Estonia.

2) Then, there are those Member States that are committed to promoting general cooperation among all states multilaterally, like Ireland or Austria, although certain states such as Romania are often lagging behind the other Member States, and therefore, require the expertise of the frontrunners because they need to catch up.

Lurking underneath are more ambient explanations: the reason why some Member States are less cooperative with each other can also be linked to their strategic cultures, which determine to a certain extent the way cyber security is being approached in the Member State. For example, in Germany, cyber security is very much driven by the home affairs section because the BSI (the German Federal Office for Information Security), which is the central IT security service provider for the federal government in Germany, is linked to the Ministry of the Interior (Schönbohm, 2012: 69). However, the BSI is independent from the German intelligence services and acts as an independent agency responsible for IT security in Germany (Interview, 2014j). Conversely, in other Member States, most notably in France but also in the UK, Romania and in many others like Poland, the national IT security agencies and national technical authorities are linked to either intelligence services or law enforcement. This latter model is slowly becoming more predominant.

Exemplifying this, in 2013, the UK government established a cybersecurity operations centre, known as the 'Fusion Cell' linked to GCHQ and MI5, at a secret London location to monitor cyber attacks against the UK and its businesses in real time (Interview, 2014j). The Fusion Cell is the hub of the Cyber-Security Information Sharing Partnership (CISP) – a knowledge-sharing forum for industry discussing

techniques used by hackers and how to tackle them –, which is part of the UK government's Cyber Security Strategy launched in 2011. At any one time, 12-15 analysts from GCHQ, MI5, and MI6 in collaboration with experts from Britain's biggest companies (e.g. KPMG, Microsoft, Lloyd Banking Group, FireEye, TechUK) will be working at the Fusion Cell to monitor what is going on in cyberspace, to get "a better intelligence picture and push it out to industry in a way that they can take action, so it is very action-orientated' (The Guardian, 2013). Furthermore, the Cyber Intelligence Fusion Cell helps monitor cyberspace in order to track down cyber attacks coming from foreign states and criminals (Lemieux, 2015). The creation of this, together with a sub-set of the Joint Intelligence Committee to offer an overview of these attacks, reflects a moment when officers from GCHQ were prominent in the Assessments Staff within the UK Cabinet Office (Interview, 2015l).

In France, the interministerial agency ANSSI (Agence nationale de la sécurité des systèmes d'information), which was established in 2009, is effectively the French national agency for computer security (ENISA, 2016a: 22). ANSSI operates with the French intelligence services and is part of the General Secretariat for National Defence and Security (SGDSN). In Poland, the National Cryptology Centre was set up jointly by the Polish Ministry of Defence and the Internal Security Agency in June 2013. In Romania, cyber security is again closely linked to law enforcement and the intelligence services. However, in Germany, cyber security is strictly separate from German intelligence services and law enforcement partly because of its historic aversion to domestic surveillance (Interview, 2014j).

While there is a widespread assumption that Member States that would like to share confidential information or perhaps think the sharing of such information would be helpful, the different cultures and mini-coalitions present a problem. A senior EU official argued that being keenly aware of the surveillance programmes in the U.S. and the UK and how the agencies collaborate, an obvious question follows: where is the guarantee that the sensitive information (linked to cyber security) shared with the Brits is not going to land on the desk of an NSA agent the next day? (Interview, 2014j). The same observation might be said about the close and over-lapping bilateral relationships between Norway, Denmark, Sweden and Finland. This implies that cyber security is a matter of trust and cooperation. However, even when it comes to collaboration between agencies, the effective sharing of information might not be feasible because the agents do not know who their counterparts are and whether they can trust them, and there is the fear that sensitive information may fall into the wrong hands – or at least different hands (Interview, 2014j).

In the NIS Directive proposed by the European Commission, there is an intriguing element regarding the application of the 'peer-to-peer'[18] review: "Within the cooperation network the single points of contact shall … (h) organise regular peer reviews on capabilities and preparedness" (European Commission, 2014). In this connection, a BSI official argued that:

Very bluntly, we (the German authorities) from the BSI, which is a civilian agency, don't want to have the Romanian intelligence service checking our sights to do the

[18] This is communication between organisations based on one individual in that organisation talking to another. Trust in this case may be more easily built up than at an organisational level.

peer-to-peer review because we don't know if there are necessarily Chinese walls[19] in those agencies, so in a way we don't trust them about the information we are sharing (Interview, 2014j).

Again, this implies that the challenges of cooperation in cybersecurity are two-fold: (1) it can be linked to the way agencies and cybersecurity generally are structured in a Member State; in other words, to the organisational culture of cybersecurity within a Member State; (2) second, it can be linked to the differences in capabilities, resilience, capacities, confidence and interests of a Member State, together with their strong bilateral connections.

Effective information sharing is a fundamental part of today's cyber security project. However, mundane technical explanations such as the different software the Member States are using can also explain why there is less information sharing. Both the EU and NATO cooperate closely and have 28 members (not the same members), and currently they are using 36 different kinds of software (Interview, 2014b). Converging one type of software, and perhaps engaging in a degree of shared training, would help in creating an environment of trust and facilitate the flow of information. However, this would also make the Member States more vulnerable technically, and so, it would be better to have common platforms rather than standard software/hardware. Therefore, it is not surprising that the strong and more developed members are reluctant to help the weaker members because if they share their best software it could be an easy avenue of attack for a potential enemy (Interview, 2014c).

[19] Chinese wall is a business term referring to an information barrier within an organisation which aims to prevent communication and the flow of information that could generate conflict of interest.

By looking at the threat landscape within the EU, it becomes more obvious why highly advanced Member States might not necessarily want to share their programmes with less developed members such as Romania (Râmnicu Vâlcea, also called Hackerville, is a hub of cybercrime) or Bulgaria because there is the assumption that these less prepared members are more exposed to cyber criminal activities (Interview, 2014j).

*Because, as **you** all know, the chain is only as **strong** as its **weakest link**.*
(Neelie Kroes, Former Vice-President of the European Commission responsible for the Digital Agenda, Brussels, 28 February 2014)

Moreover, as another EU official observed, if a highly advanced Member State invests heavily in cyber security, presumably they do not want others to 'free ride' on what they have been doing (Interview, 2014j). Avoiding the free riding culture is a balancing act as it is important to ensure that the weaker Member States are not lagging behind and are able to catch up since their vulnerability means that ultimately there is a vulnerability in the union which represents a backdoor that can easily be 'kicked down'. In economic terms, these states often look like free riders in a cartel such as the Organization of the Petroleum Exporting Countries (OPEC).

Trust is a vital issue among the Member States and there have been reports of Member States hiding details of the development of cyber offensive capabilities from each other, which could result in a lack of collaboration when it comes to trust-building and information-sharing measures, since defensive co-operation can reveal vulnerabilities. Peter Round, Director of Capability, Armament and Technology at the EDA argued that:

One of the issues with cyber is that it is in some ways the new gunpowder. When a

Member State gains a capability – certainly at first – they don't want to share it, because some have it and some don't, and we are seeing that some don't want to share it, seeing it as a sovereign and national issue (Fleming, 2015).

Compared to the U.S., much more could be done to facilitate Public-Private Partnerships in the European Union. To illustrate, the National Cyber-Forensics & Training Alliance (NCFTA) that is based in Pittsburg is an entity where representatives of 80 private organisations and more than 15 U.S. and international law enforcement authorities work on cybercrime cases under the same roof. They are backed up by the research and brainpower of the world famous Carnegie Mellon University computer science lab. This is a prime example of what the synergies of law enforcement, private sector and academia should be. However, this level of integration and synergies between law enforcement, the private sector and the academic world does not seem to be possible in Europe because according to a Europol officer it still operates with a silo-mindset (Interview, 2015i).

5.5. Different levels of preparedness

How much countries are willing to invest in cyber security depends on the threats they are confronted with and the general economic situation. Budget is always subject to priorities and depends on what is at stake at that moment in time and what policy is a top priority. For instance, if a country has lots of economic issues and social tensions such as Greece, then cyber security might not be an urgent priority. However, for countries with highly connected industries like Germany and the UK in which the economy depends on these industries in terms of GDP (because they provide taxes) then it is understandable that cyber security is a vital policy issue. This is part of the varying economic structures that all EU Member States are subject to, with the UK and

Germany having undergone the most "financialisation' and therefore setting the highest priority on protection of the e-economy.

Moreover, the extent to which Member States invest in cyber security can be also linked to the way a country's government understands the problem and how it articulates to the public the reality of the growing and significant threat posed by cyber attacks, together with their impact on society and the economy as a whole. The way the political elite understands the problem is often linked to historical experiences in the past with national security threats. Furthermore, the technical situation can be also a vital factor in determining to what extent a country considers cybercrime a leading threat. For example, some Member States have less advanced technology and limited broadband coverage, therefore, SMEs or large industries in that country may not be up-to-date in terms of their linkage to the Internet and how to use IT systems, and this might be another reason why a Member State does not consider cyber attacks as a vital threat to the nation.

According to an EU cyber policy adviser at the European Parliament, another major difference between the U.S. and EU approaches to cyber threats can be linked to the extent it is dominated by government agencies (Interview, 2014j). Whilst the U.S. is very much focused on a close exchange with experts from both the academia and the private sector/industry, however, in the end, policy is still strongly dictated by government agencies. For instance, the U.S. Presidential *Executive Order 13636*, *Improving Critical Infrastructure Cybersecurity*, issued in February 2013, directed NIST to develop a framework for reducing cyber risks to critical infrastructure.

Although this is based on an exchange between industry and the government, ultimately, it is still strongly dominated by the Executive.

The differential sophistication of the development of ideas could be another reason why Member States have different cyber security preparedness. The EU recommendation is that all Member States should have their own cyber security strategy. This policy area is relatively new, so this might be a question of evolution since we are still in the embryonic stages at the national level. Having said that, not all Member States signed up to the Budapest Convention (at least five haven't signed up yet), which would be an obvious step they could take (Greece, Ireland, Luxembourg, Poland and Sweden are reportedly about to ratify it).

On the EU level, it is not necessary for all Member States to spend money on replicating their systems, if we are able to achieve some kind of network contacts when there is a cyber attack, for instance, or when all the lights go out across Europe. Therefore, it is important for all Member States to establish their own CERTs, and to enhance the level of cooperation between CERTs and law enforcement entities in a common fight against cybercrime both in the EU, and also cooperating with the U.S. as much as possible (Interview, 2014f).

A good example of successful international cooperation is the 24/7 network of cyber investigators which was established among the G8 nations in 1997. The G8 Summit is another forum in which EU-U.S. cooperation has been advanced. As a result of Russia's aggressive annexation of Crimea, Western powers shifted their G8 summit in Sochi to a G7 meeting in Brussels. The previous G8 summit was hosted in the UK,

under the UK Presidency; some good progress was made on 24/7 networks and some initial thoughts on the impact of Big Data and how that could be used for common use. Unfortunately, with recent developments, the G8 has lost its momentum (Interview, 2014f).

6. Conclusion

Within the Internet context, economic growth is clearly a shared interest for both the EU and the U.S., however, the strategies designed to protect these economic interests are developed in different ways. Both the EU and the U.S. naturally aim to maximise their own interests. Furthermore, we are dealing with strategies, which stem from cultural traditions in which certain values/morals develop that may look universal but are in fact open to much local interpretation.

Differences in definitions matter when it comes to common terms and strategies – co-operation is therefore a balancing act. For instance, as the EU sees human rights as universal, the protection of human rights is not dependent on nationality. So, a U.S. citizen could claim a breach of the European Convention on Human Rights stemming from the actions of one of the parties to the Convention. By contrast, the U.S. constitution and its amendments do not offer protection for non-U.S. citizens. This became clear in the Schrems case, when actions of the U.S. government would impede on the interests of EU citizens, yet these citizens do not have legal address before a U.S. court stating a breach of constitutional rights. (Interview, 2016e).

If the economic value is a common shared interest, then why are the EU and the U.S. often so divided? One suggests the reason is that all the stakeholders still play in a competitive rather than in a collaborative way.

Paradox: there is a need for legislation because the "tragedy of the commons" teaches us that every common space will inevitably be overused and ruined because the users have competing interests and there is no technical solution, no objective mechanism that will tend towards a balance; it remains dependent on the interest of users. In other words, it won't settle on natural equilibrium. The digital space will continue to be exploited and that is why it needs to be regulated. However, it is hard to create legislation that brings about much needed balance - it has to be balanced regulation: soft law that needs to be implemented (Interview, 2016e).

According to an EU cyber policy advisor at the European Parliament, one of the biggest obstacles to transatlantic cyber security collaboration is not technical or organisational but the *human element* (Interview, 2014j). After the Snowden revelations and the whole surveillance issue, trust has been severely damaged at the political level. Therefore, the question was often raised as to what extent the EU is able to trust her transatlantic counterpart and invest in this partnership?

Notwithstanding this, the EU and the U.S. have been collaborating closely on cyber security and in the fight against cybercrime. The main reason why the EU treats the U.S. as its most vital partner in cyber security is because they share similar values strategically and agree on many of the fundamentals of Internet governance – seeking to keep it open and free yet secure. Fighting cyber crime in their own jurisdictions is

the most obvious field of cooperation, but the ultimate goal is to reach out to the weaker nations that are trying to catch up. In the short term, this might present a problem. For example, relations with China will present serious challenges. Yet despite the fact that China represents a different value system regards to cyber security by blocking foreign tech companies such as Facebook, Twitter and Google from the Chinese domestic market, Lindsay argues that a cyber war between the U.S. and China is highly unlikely since there are strong U.S. economic interests at stake (Lindsay, 2015:9).

In a similar way to China, Russia has a completely different approach to Internet governance (IG). Russia regards cyberspace as a territory with virtual borders corresponding to physical state borders and wish to exert sovereignty in cyberspace and regulate Internet content within its borders, which would not only lead to a certain fragmentation of the Internet but also would see the rise of state authority on the Internet – something that the Western world would like to avoid.

This chapter has focused on the EU-U.S. challenges and approaches to privacy and cybercrime. It argued that there are many differences and obstacles on the strategic-legal level compared to the operational level. For example, digital evidence gathering in cybercrime investigations is a slow and cumbersome process compared to the operational level where intelligence gathering is smooth and efficient. Illustrating this, the BlackShades case demonstrates a successful investigation where prosecutor-investigator collaboration was well coordinated. The case studies suggested that the power of corporations cannot be ignored in transnational cybercrime investigations as they possess vital information, technical expertise, and threat intelligence, and

therefore, unsurprisingly, both law enforcement officers and prosecutors have to rely on them increasingly. This also reflects the relative weakness of states and a tendency of technology - not politics - to shape the future landscape.

To answer the question of finding the golden balance between privacy, security and surveillance with regard to cyber remains challenging. Cyber security is larger than any stakeholder can alone manage. Politicians, law enforcement and intelligence officials asking to weaken security systems and aid surveillance in order to spot and disrupt cyber criminal and terrorist activities cannot be executed without the expense of personal privacy. Harmonising activities and working cultures between the public and secret sphere might be the solution in creating strong transatlantic strategic cyber cultures.

Chapter VI.

Conclusions and policy recommendations

1. Recognising the problem and main lessons learnt

Overall, this research provides empirical evidence of applying strategic culture in the EU-U.S. cyber security context. The reason why the transatlantic partnership is the main focus of this thesis lies in the fact that both the U.S. and the EU are at the forefront of shaping cyberspace; meanwhile transatlantic cyber crime cooperation has been one of the most successful platforms. The methodology draws on notions of strategic culture. This research tests the extent to which different mind-sets, rooted in strategic culture, can be regarded as an obstacle to develop trust when collaborating among various stakeholders across the Atlantic. Strategic culture is a prominent factor and acts as a vital tool in order to achieve a more nuanced picture of the drivers of strategic cyber cultures by examining the problems that have arisen in EU-U.S. collaboration in the fight against cyber crime.

While this subject represents an advanced case study, surprisingly there is still no current literature written on cyber crime from a strategic culture perspective. Therefore, the concluding chapter is going to be structured in the following three ways: 1) main comparative lessons based on the policy/strategic, legal and operational components of strategic culture as well as policy recommendations; 2) addressing broader implications (conceptual as well as empirical); and 3) future research directions.

First and foremost this research highlights that any policy, strategy or research on cyber security and cyber crime needs to address the lack of a universal definition of cyber security and cyber crime. Both terms are quite vague and are used to define complex areas of public policy. Since the dynamics shifted from the technically minded community into the realm of public policy and national security, an increasing number of stakeholders has become involved, each bringing with them their own conflicting interests and ideas. This has increased the challenges and complexity for those already operating in the cyber security setting (Van der Meulen *et al*., 2015: 113). The fact that cyber crime means different things to different stakeholders leads to fragmented cyber strategies. Also the way the issue is framed and understood by state and sub-state entities has an impact on what is considered a cyber threat as well as the strategies, responses and measures that are implemented at the strategic, legal and operational levels. These different attitudes and approaches lead to fragmentation and are aggravated by the absence of clear definitions. The problem of definition is a practical one that cannot be ignored when trying to generate collaboration in the fight against cyber crime.

Second, this thesis aims to highlight the constant changes in EU – U.S. strategic cultures reflected in the transformation of attitudes, mind-sets and foreign policy behaviour by creating a better understanding of where joint efforts are possible given the different cultures at work. According to Jeffrey Lantis, such phenomena generally occur when an external shock or recent historical event impacts the manner in which the security community executes strategic decisions and responses (Lantis, 2002: 111). As such, some scholars argue that without a 'cyber Pearl Harbor' or another form of external trigger, there is unlikely to be significant change to the current

transatlantic cyber status quo, which might help to alleviate the fragmentation of strategic cyber-cultures and enhance its unification across the Atlantic (Bisson, 2014: 57).

To repeat, this research argues that there is no single or monolithic strategic cyber culture abiding in the EU and the U.S. therefore, it is suggested that the deployment of the concept of strategic culture requires some expansion or elaboration. In other words, it needs to include the various organisational sub-cultures of those agencies and bodies that act as vital players in the formation of EU-U.S. approaches in the fight against cyber crime. Accordingly, this research proposes that there are many strategic cultures present in the cyber security field, therefore, strategic cyber culture needs to be examined at three levels: (1) strategic/political (2) legal/regulatory and (3) operational/military dimensions.

By broadening the concept of strategic culture this facilitates a better understanding of elite decision making on cyber security policies in this complex domain. It is necessary to acknowledge that because the EU is a politico-economic union and the U.S. is a collection of federal states, it is difficult to effectively display differences between these two bodies in terms of their response to cybercrime, leading to complex methodological issues. Different cyber cultures elicit different strategies and responses. However, the U.S. displays more cultural unity due to its federal structure and its longer existence as a union than the EU. In contrast, the EU's strategic culture could be characterised as an agglomerated culture at the supranational level with a

"margin of appreciation" [20] for its Member States (Greer, 2000: 5). The methodological difficulty lies in determining whether these differences are present on an executive, political, national, public agency or EU and federal level. In addition, another limitation of this thesis is finding a way to illustrate the differences between these layers, i.e. between the political sphere, the public sphere, the agency sphere and the institutional sphere.

Third, the thesis proposes that historical experiences with cyber security related threats in the past play a vital role in terms of codes of conduct, threat perceptions and technical developments of a state, sub-state (or non-state) actor to address cyber threats - often in conjunction with the private sector that owns most of the data needed to effectively combat cyber crime. During the Cold War, economics and politics were largely polarised between the communist and non-communist world, presiding first over episodes of nuclearisation and then denuclearisation. Today's digital era however, is very different and non-polarised. Moreover, in cyber security there is no clear formula to deliver only privacy or only security, and in any case most entities prefer to maintain a quest for both - privacy (the right to private communication) and to keep the criminals and terrorists out. This all contributes to fragmentation and many "overlaps" between the EU-U.S. strategic cyber cultures at all levels, including policy/strategic, legal and operational frameworks.

Fourth, the thesis exemplifies in the case study chapter that EU – U.S. divergences on the policy and legal levels are more distinctive and create a 'strategic dissonance' when prosecuting cyber criminals that is in sharp contrast to the convergence and

[20] According to Greer "The margin of appreciation" refers to the space for maneuver that the Strasbourg institutions are willing to grant national authorities, in fulfilling their obligations under the European Convention on Human Rights (the Convention)" Available online at http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf

efficiency of collaboration at the operational/executive/security services level. Demonstrated in the Blackshades case study there is clearly much more convergence in collaboration at the operational level, where there are similar attitudes. Comparatively, attitudes at strategic or legal stages can be counter-productive, and frequently hinder inquiries.

The challenge for the EU is that strategies - including the EU's Cyber Security Strategy - are established at a very high level and therefore need to be generic and are dependent on the implementation of the 28 Member States respecting the "margin of appreciation". When developing EU strategies, it is essential to minimise differences. Where the harmonisation of legal frameworks is not attainable, then work processes should be harmonised. In fighting cyber crime, a classic approach is for law enforcement to dominate. However, this is too one-sided. Certain behaviour would indeed be classified as criminal but other "criminogenic" factors that could influence someone to become a cyber criminal would be omitted by this one-dimensional approach. Accordingly, an integrated approach is more desirable, whereby other stakeholders including governmental bodies or private entities can intervene to address criminality. In other words, a more integrated approach could help to provide redress to victims and restore public order. Public-private partnerships are possible alternatives to the criminal justice approach and these are more common in the U.S. than in the EU, albeit this strategy is well established in a few EU Member States (for e.g. in the UK). In other EU states, legislative difficulties might arise, especially where national law enforcement is not allowed to share information with other parties.

EU:

The EU Cyber Security Strategy (2013a) and the NIS Directive (2013c) encapsulate the EU's approach to cyber security. The EU chapter within this thesis examines in some detail the institutional structure and the main entities that are responsible for the EU's strategic cyber culture: DG HOME, DG Connect, ENISA, EC3, EDA and CERTs. EC3 and Eurojust are the main players in the fight against cyber crime and work as facilitators and coordinators. Furthermore, EC3 also plays a vital role in providing strategic analysis about recent trends and methods of criminal activity to EU policymakers and Member States.

This thesis highlighted that even within an organisation, the remits of agencies in the fight against cyber crime are often unclear and sometimes confusing. One of the contradictions noted by an EC3 official was that despite the fact that it is essential for EC3 to measure the vulnerabilities of CIs that can directly influence the work of EC3's three Focal Points, the NIS Directive this year gave no role for law enforcement. 'The original version of the NIS Directive asked for non-mandatory report to law enforcement that has been left out and the current text will not be changed' (Interview, 2016e). In many countries, the business of critical infrastructure protection is a shared role between the state security service and the national CERT (ENISA, 2015).

U.S.:

Compared to the EU, the U.S. has a much longer and more complicated history of activity in the field of cyber security. Although the Computer Fraud and Abuse Act goes back to 1984, 1998 could be considered the watershed year when the U.S.

government began to take cyber security risks more seriously. Like in the EU, there are various entities that could be considered the main carriers of U.S. strategic cyber culture. However, they often do not have a clear understanding of their role and often generate overlaps. Whilst the DHS focuses more on civilian aspects by protecting federal networks, the FBI is considered the leading agency for cyber crime issues. Nevertheless, the capabilities are distributed among yet other agencies such as the USSS, creating further challenges regarding mandates. However, an FBI agent recently confirmed that coordination efforts have been improving in the area of cyber crime (Interview, 2016b). The DoD is also a major player in U.S. cyber security and focuses on cyber defence. USCYBERCOM is part of the DoD and was established in 2010. The recently published (April 2015) DoD cyber strategy has been more open about advocating offensive capabilities and deterrence, naming potential enemies that pose a threat to U.S. national security. Some researchers have noted the emergence of new players in the U.S. cyber security field and argued that allowing too many institutions to participate only complicates the U.S. cyber security landscape. With almost 62 federal office "overlaps", the allocation of resources and responsibilities regarding who has to do what, when and how, becomes a highly problematic issue (Van der Meulen *et al*., 2015). These differing views and approaches to cyber security underline the fragmentation in U.S. cyber culture strategy among the various entities. Therefore, the EU need to learn from this lesson and to be careful about introducing new entities into its cyber arena is it wishes to avoid the same fissiparous texture.

Policy recommendations

The importance of EU-U.S. collaboration in the fight against cyber crime has been recognised by both sides and child sexual exploitation is one area where cooperation

is strongest. This thesis attempted to highlight the challenges of transatlantic collaboration at the strategic, legal and operational level in the hope that collaboration can be extended further.

Some of the concerns include:

1. Member State competent authorities lack the legal scope to target servers hosting child sexual exploitation (CSE) material and to establish server programmes that would allow them to seize control of the server. Therefore, more cyber-specific investigative powers and approximation are needed at the EU level.

2. Cooperation with the private sector is essential for the government bodies and law enforcement agencies. From breaking encryption in cases of imminent terrorist attacks, to taking down botnets, to improving the cyber security for both the U.S. and the EU – these aims cannot be achieved without the private sector which often boast greater resources and stronger expertise than state agencies.

3. *Encryption:*

   The ability to monitor electronic communications is decreasing with each new encryption tool provided on communication platforms. Still, such data is absolutely critical to identifying everyday criminal activity such as kidnapping, fraud, child pornography and exploitation, among many others. FBI Director James B. Comey has criticised the increase in the use of irreversible encryption introduced by big software companies, which makes it impossible for the law enforcement agencies to tap into communications and gather online evidence.

In the U.S., a law passed in 1994 obliges traditional telephone companies (the Communications Assistance for Law Enforcement Act (CALEA)) to have systems that permit government access through a court order. However, emails, chat and instant messaging are not covered. There is an on-going debate in Congress about whether the CALEA should be updated, although it is doubtful that a law allowing government access to encrypted communication would pass Congress. There is a similar situation in the EU where it is also very cheap to encrypt and very expensive to decrypt. As a consequence, other measures may have to be explored such as greater use of legal interceptions instruments such as malwares and key loggers. We will also see a greater exploitation by government of meta-data for intelligence purposes, albeit this is not as useful as evidence in court.

The counterargument is that creating regulations and laws that force companies to create an entry into any system for the government, or "backdoors for governments", will also open up an avenue for cybercriminals. This is the "going dark" problem of IT corporations: they implement stronger encryption measures as a way to create safer security systems for users but preclude the government's ability to obtain such information, even with lawful court-issued warrants. Apple has cleverly articulated its new encryption system as an anti-government tool to thwart court-ordered interception, which some see as a provocation to garner more public attention and publicity.

Compounding the problem is that fact that the Snowden leaks of 2013 increased public perception that the intelligence community has too much, not too little, access

to information. For law enforcement, which is generally years behind the intelligence services in terms of capability and capacity, this is causing several problems in tackling criminal threats. On the strategic level, law enforcement faces an uphill task to make the point to the general public that, in fact, full encryption can also be dangerous for society in terms of their everyday work against cyber crime.

With smartphones and "big data", the traditional Fourth Amendment line is becoming obsolete (i.e. prohibits unreasonable searches and seizures and requires any warrant to be judicially sanctioned and supported by probable cause). The reality of electronic communications is here to stay and is playing an increasingly pivotal role in committing crime. The ability to monitor electronic communications is therefore essential, once it meets the necessary Fourth Amendment standards and any other fundamental rights (right to privacy etc.).

An alternative option is called "compelling disclosure": enacting laws that oblige suspects to reveal their passwords with penalties up to 30 years of imprisonment if they refuse (UK, Australia, Canada, FR, India and other countries have such laws in place). However, this raises issues such as the "privilege against self-incrimination". In Europe the jurisprudence is not clear but there is an expectation that very soon the ECHR in Strasbourg will produce a ruling supporting compelling disclosure. Until then, the principle is open to interpretation.

4. *Mutual Legal Assistance Treaties (MLATs)*

There is a wide consensus that MLAT clearly needs to be reformed due to the current time constraints imposed by this slow procedure. However, there are two opposing

camps: while law enforcement authorities want to speed up the process (emphasising the volatility of digital evidence), the data privacy community and civil liberties advocators want to protect users with additional safeguards. This suggests that MLATs won't be reformed any time soon. For instance, if the server or the perpetrators are based in a jurisdiction (Russia) that is not willing to cooperate, then the cyber crime investigation is blocked because EU Member States rely on MLATs that are not taken or observed by these foreign jurisdictions.

The reality is that the MLAT process is an old fashioned legal instrument that is ill-suited to the realities of 21st century cybercrime. The U.S. has informally decided to no longer answer MLAT requests from individual countries because the DoJ is simply flooded with MLATs coming from all over the world. In short the system has broken down.

The question then arises whether it is possible to work without MLAT. The question of unilateral access by the law enforcement agencies of one state to data stored in/on a computer system in a foreign state without the need for MLA has been a topic of discussion since the 1980s. *Article 32* of the Budapest Convention on Cyber Crime attempted to solve the MLAT problem but was unsuccessful because there was no workable consensus among the parties. Article 32 of the Convention provides that:

> a party may, without the authorisation of another party (i.e. without MLAT) a) access 'publicly available' (i.e. open source) stored computer data, regardless of where the data is located geographically (This is limited in use because only open source information is concerned) or b) access or receive through a computer system in its territory, stored computer data located in another party if the party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the party through that computer system.

In other words, it refers back to the MLAT solution, as there are no other means available to obtain such consent - so the Budapest Convention is not effective in that sense.

Other commentators argue there is a need for a "paradigm shift" and a global consensus among prosecutors, magistrates and law enforcement agencies prosecuting cybercrime that gives direct access to data in foreign jurisdictions. In other words, if you can see evidence from your computer in your office in the UK or in The Netherlands, it should be permissible to seize (copy) it for use in court, regardless of where the server is located. Some countries are adopting this type of legislation. The best example is Belgium: Article 88ter of the Belgian Criminal Code of Procedure "allows investigative judges[21] when he orders a search in a computer system, to extend the search to another computer system or to a part of another computer system located elsewhere" (Kerkhofs & Linthout, 2013: 6). The Belgian approach offers a flexible solution to handle data stored in the cloud and to secure digital evidence based on where the data is accessible, as opposed to where it is stored. Other countries such as the The Netherlands and Portugal are taking a similar approach.

According to a Eurojust cyber crime prosecutor, there is a need for a two-fold solution where the working procedures of law enforcement and prosecutors are aligned. This is called "MLAT – streamlining". On the legislative side, the current legal framework does not allow for expedited transfer of evidence. This provision is lacking in treaties with the U.S. However, it is possible to freeze evidence. In comparison, in the EU expedited transfer of evidence works well (Interview, 2016e).

[21] "This is a Judge with special duty to lead the investigation and with special investigative powers" Kerkhofs & Linthout, 2013: 6) Available online at *Belgian jurisdiction in Cyberspace*

The next problem is to get Internet Service Providers (ISPs) to cooperate with investigators. Private firms frequently hide behind the absence of MLAT and argue that the law in the country where they are based does not allow investigators to seize evidence or allow them to reveal real IPs. The Yahoo! case demonstrates this problem: a Belgian prosecutor requested Yahoo! (in an email) to provide data related to two individuals who committed fraudulent activities in Belgium through Yahoo! email accounts (Pollicino & Romeo, 2016). Yahoo! refused to fulfil the request, arguing that since Yahoo! is not physically based in Belgium, it has no legally binding obligations towards Belgian investigations and therefore the Belgian prosecutor has to use the U.S. – Belgian MLAT (Pollicino & Romeo, 2016). The case was ultimately decided in favour of Yahoo! by the Ghent Court of Appeal and then the Court of Cassation of Brussels (Pollicino & Romeo, 2016).

Several law enforcement officials and cybercrime prosecutors confirmed that U.S. privacy laws allow U.S.-based service providers to voluntarily give up non-content data if there is a direct request. However, in practice, each electronic service provider (ESP) has their own procedural requirement, which hamstrings transatlantic efforts. The reality is that ESPs dictate the procedures that need to be followed, and strictly speaking, they dictate which jurisdiction is applicable and indeed where law enforcement can operate

Here the solution may be to adopt national legislation saying in substance that if a company offers a service in country A, regardless of where it is based (e.g. country B), it must be prepared to also abide by the law of country A. This would include for

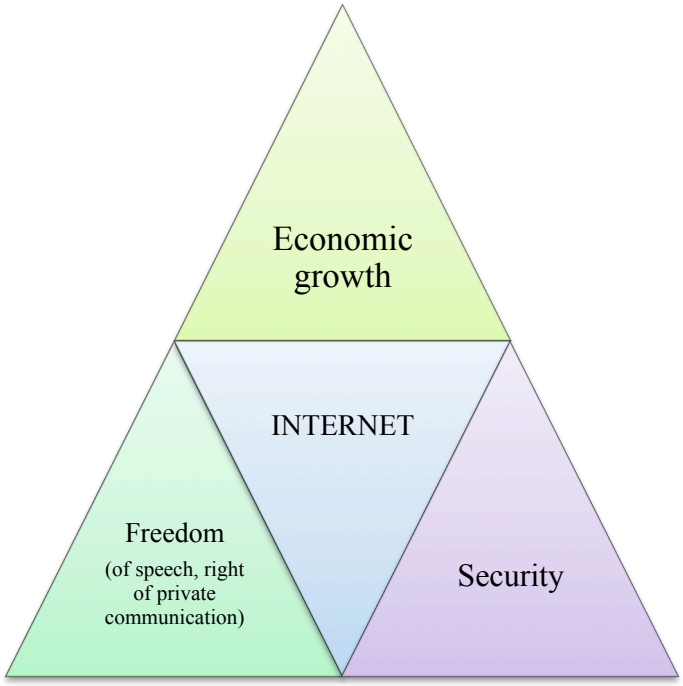
example, the obligation to accept search warrants and subpoenas and reveal IPs to law enforcement agencies. This approach was taken by the DoJ against Microsoft when a criminal search warrant was issued requesting all content-related information from an email account stored in the company's servers in Dublin (Sheftalovich, 2016).

It is suggested that the EU-U.S. should adopt similar legislation on the basis of this principle, to resolve the current problems with MLATs - the FBI could then access evidence in servers in Europe if needed, and the EU police would do the same in California. This would be a mutual collaboration. In the short term and alternatively, the MLAT process could be "industrialised" in order to keep up with the pace of cybercrime investigations, but this would require specific commitments from the DoJ at the political level. For this solution to work, strategic partnerships would need to be established with trusted partners who agree to work without MLATs or to give priority to MLAT requests coming from this limited group of trusted partners. EU-U.S. cooperation should be the backbone of this initiative.

Europol/EC3 is trying to achieve this (speeding up MLAT between EU and US) by having a U.S. DoJ Attorney placed at EC3 to work closely on MLATs coming from the EU to the U.S. and visa versa. JCAT could also speed up operations by using JITs and allocating a prosecutor to each case from the U.S. who could produce MLATs on demand because investigations are carried out jointly. But this is a transatlantic solution and ignores the fact that cyber crime is a global issue.

2. Broader implications of strategic cyber culture

Most importantly, strategic cyber cultures can be shaped and influenced by the three main pillars of the Internet: economic growth, freedom and security. These three pillars are effectively competing factors, and if there is an over-emphasis on one value, it will "override" the others and create imbalance. Each pillar wants to pursue and maximise profit and value, but mathematically it is not possible to maximise each variable simultaneously. As such, the balance point is likely to have a sub-optimal outcome (this is called the Nash Equilibrium in competing games/game theory or the Cooperative Equilibrium in cooperative games) (Interview, 2016e; Mailath, 1998).



[Figure 6.1.]: *Pillars of the Internet*

In other words, strategic cyber culture also depends on the angle/pillar from which we view cyberspace: (1) from a security perspective, cyberspace is often considered to be the 5th domain of warfare, so maximising security is paramount; (2) from a civil liberties angle, cyber culture maintains the freedom of the Internet; and (3) from an economic angle it is all about sustaining economic growth and e-commerce (for e.g.

World Economic Forum). In order to understand the moral codes that underpin the actions of the other party, it is important to consider these values in the correct context. State and sub-state actions and responses originate from a system of beliefs/morals that is different to other parties. Ideally, any strategy that is implemented by governments will achieve a balance between these competing values. However, some of the variations in interpretation of these values in the U.S. and EU are analysed in this thesis. For instance, privacy is perceived differently in the U.S. (consumer-protection rights) compared to the EU (fundamental right, reasonable expectation) (Whitman, 2004: 1157). These differences highlight that actions and policies originate in differing systems of beliefs and morals.

Similarly, economic growth is a shared interest for both the U.S. and EU. However, they differ in terms of how strategies are devised to protect their respective economic interests. The U.S. focuses much more on IP protection than the EU (Interview, 2016e). However, the economy has geographical boundaries, unlike the Internet, which is not territorial. Companies that have their headquarters in the U.S. are bound by U.S. laws. This is evident, for instance, in the fact that data stored outside the U.S. by a U.S company may still be subpoenaed under U.S. law. However, after the old Safe Harbour Agreement was annulled by the ECJ in October 2015, a new political agreement called the EU-U.S. Privacy Shield was implemented in February 2016 to legislate for the exchange of personal data for commercial purposes (European Commission, 2016, IP/16/216). Its authors assert that the new framework fully protects the fundamental rights of EU citizens when their data is transferred to the U.S. (European Commission, 2016, MEMO/16/434).

The U.S. State Department is at the forefront of trying to establish and promote common norms of behaviour in cyberspace that are considered the "basic building blocks" of co-operation, designed to minimise cyber security issues (Farrell, 2015). Intriguingly, sometimes Pentagon officials also argue for this approach rather than for hard military tools. Admiral Michael S. Rogers (head of the NSA and Cyber Command) called publically for the support of academia and civil society in the development of shared cyber norms at a recent cyber event (Rogers, 2015). Nevertheless, in order to achieve this aim, legal scholar Margo Schlanger argues there is a need for a radical reset of the strategic cultural mind-set of the military and intelligence community (NSA, CIA, Cyber Command) by leaving "intelligence legalism" behind and abandoning operations that contravene the norms the U.S. intends to create (Schlanger, 2015). In other words, the public statements of intelligence officials that they abide by the law are not sufficient, because their understanding of the law is often influenced by "secret interpretations" that exceed legal constraints (Farrell, 2015).

The thesis highlighted the differences between how the U.S. and the EU intends to regulate the Internet. Given that economic value is a shared interest, then there are some puzzling questions about why the EU and U.S. are so divided. One of the reasons could be that they both operate in a competitive rather than collaborative manner with regards the three values (freedom, security and economic growth). If you have more than one value dependent on other things linked to each other then it is impossible to maximise all three values and at the same time and a balance is needed. The optimum is always less than the maximum. Both the EU and U.S. try to maximise their own interests. Moreover, cyber security strategies stem from cultural

traditions in which certain values/morals develop that may look universal but are subject to a certain amount of interpretation.

Furthermore, differences in definitions matter when devising common terms and strategies. For instance, since the EU recognises human rights as being universal, their protection is not dependent on nationality. So, a U.S. citizen could claim a breach of the European Convention on Human Rights based on the actions of one of the parties to the convention. The reverse, however, is not true: the U.S. constitution and its amendments do not offer protection for non-U.S. citizens. This became clear in the Schrems case. Where the actions of the U.S. government infringe the rights of EU citizens, there is no legal redress before a U.S. court addressing a breach of constitutional rights (EU Court of Justice, 2015).

Since there is so much interdependency between the various entities and actors, nobody can exert control over the entire Internet. If an actor focuses solely on control through regulation, then the power of the Internet is diminished by making it less free and less innovative. In essence, autonomy, which is the driving force of the Internet, is undermined. Or if an actor focuses solely on prohibition (for e.g. on cyber crime laws), then user behaviour becomes restricted and it is likely that laws based on prohibition will lack balance between the three pillars of the Internet. If there is the capability to enforce the legislation effectively then an optimum situation/balance of the three pillars might be achievable. However, in the end, law enforcement rarely has enough traction and in itself cannot make the Internet secure, free and economically viable at the same time.

Paradox:

Garrett Hardin's expression of "the tragedy of the commons" (published in *Science* in 1968) teaches us that common spaces are doomed to be destroyed because their users have competing interests (Ostrom, 2015: 2). There is no technical solution, no objective mechanism that will tend towards a natural balance, and therefore it remains dependent on the interest of users. In other words, self-regulation has its limits and will eventually prove insufficient to prevent the destruction of the common space. Therefore, according to a senior cybercrime prosecutor at Eurojust, there is a need for legislation that both enforces and protects. However, it is very difficult to create legislation that brings about this much-needed balance. "It has to be a balanced regulation - soft law that needs to be implemented" (Interview, 2016e).

Further criticisms that emerged from the interviews were that current cyber security strategies are still focused on the short term, are geographically limited and based too much on the ethical codes of their respective regions. For genuine cooperative work, a long-term strategy is needed that is based either on true universal rules values or at least on the common ground that exists between the different parties. For instance, in Japan online child sexual exploitation still exists and was condemned by the UN after an investigation, despite the fact that Japan ratified the Budapest Convention on Cybercrime (Interview, 2016e). In short, there is a danger of creating legislation that is too generic in order to satisfy all parties. A sense of urgency is clearly needed – but based on a collaborative effort and not a competition.

Since the current rules in cyberspace are based on competition between different players, interests and strategies, the end result is that no one is content. This is clearly

demonstrated by the example of the Safe Harbour case and the divergent views between the EU and the U.S. on data protection. In contrast, a collaborative game has different perimeters/rules where one needs to objectively appreciate the position of the other party. If this is not the case, then every negotiation is "coloured" by the interest and strategic cultural mind-set of the respective parties, when ideally it should be based on the optimum[22] level of the value of all parties.

3. The road ahead

Cyberspace is undoubtedly a highly complex environment in which all the different players involved - regardless of whether we are referring to states, sub-states or non-state entities - contribute their own cultures and attitudes, yet are often lacking a clear understanding of what they wish to achieve. Therefore, there are tremendous opportunities to do further research on cyber security, especially in the fight against cyber crime. In the shadow of Snowden revelations, both the public and the private sector have taken advantage of the tendency towards greater use of end-to-end encryption in communications however, it still leaves a blurry line of what role the government and law enforcement can play in order to carry out investigations on crime and terrorist activities online. Finding a workable solution and compromise would be essential. Furthermore, there is also a lack of harmonisation of approaches regarding the regulation of the increasing use of cryptocurrencies (used by cyber criminals) such as Bitcoin that could be another direction for future research (Europol, 2015b: 99). Similarly, research could be carried out on how EU-U.S. best practices in

[22] An optimum value in a collaborative way is higher than the optimum value in a competitive way (but can only be achieved if all players have all available information at their disposal – without that, it is unlikely that an optimal cooperative equilibrium will be achieved).

increasing cyber security and combatting cyber crime could be disseminated and developed in other regions of the world.

Complaints have been made by various stakeholders about the "all talk, not enough action" work ethic, which often characterises both formal and non-formal cyber security meetings, conferences and workshops. Simply identifying and discussing the problems of cyber security and emphasising the importance of collaboration is clearly ineffectual if such discussion is not followed by tangible action.

Both the EU and U.S. will continue to face similar challenges where boundaries between terrorism, crime and protest will blur. This will be boosted by the facility and ease with which you can become a cyber criminal. Cybercrime is like a service now – you can go to a website and for a small fee, purchase a DDoS cyber attack on your competitors' websites or you can buy credit card numbers. It is all easy, cheap and accessible. Grams, a new search engine modelled on Google, allows users to search the Tor and Dark Web sites, which makes it possible for criminals to buy drugs or weapons online (Buxton & Bingham, 2015: 5).

Using cybercrime to fund terrorism is a high profile issue, but a new phenomenon has emerged, namely "hacktivism", which is hacking to promote social and political causes. For example, the anonymous taking down or defacing of websites. Unlike cyber terrorism, hacktivism is not focused on creating a sense of fear or horror. Some communications studies experts suggest that this will become the political mainstream. It hasn't happened yet but it could happen: for example, instead of al-Qaeda attacking a power station where all the lights go out, green activists might launch a denial of service attack on the House of Commons.

Brazil is a cybercrime hotspot, and recently there has been a dramatic increase in the number of botnets and malicious codes emanating from here. Security researchers discovered that criminals were writing in a particular code language that wasn't taught in the universities but was taught in vocational training colleges, so people from the lower social scale were able to access these codes and take the opportunity to commit cybercrime. Today, almost 3 billion people are online and this will increase to 4.7 billion in the next 10-15 years. As 75% of these people will be from developing countries, the market for potential criminals and also for potential victims will significantly increase.

A further challenge is that law enforcement is a "nation-state" phenomenon, particularly in the context of EU competence. Ex-third pillar, the European Commission has no real voice here. There is also the problem of jurisdiction as law enforcement agencies are only authorised to enforce the law within their jurisdictions. For example, if a Dutch police officer is online asking to raid the home of a potential cyber criminal in France, currently, the legal framework would not allow that. Jurisdiction is a major issue and the lack of agility with which an investigator can request information or access evidence is problematic.

To conclude, in an ideal world we would devise a Kyoto agreement for the Internet - a model international treaty that defines acceptable behaviour in cyber space. It would constitute a norm-setting agreement regulating the actions of both nation states and individuals on the Internet. Such a global agreement could then be used to establish common frames for an EU-U.S. agreement on how various stakeholders including

government agencies, law enforcement agencies and private entities are allowed to operate and under which conditions. However, that is not a quick fix, and the Snowden revelations have delayed the prospects of this wider solution. There is also currently no world consensus for this kind of global solution. China and Russia are manoeuvring the UN to undermine the Budapest Convention; so talking about a global agreement is probably too optimistic. While global governance remains weak, the struggle against cyber crime remains a troubling task for the officers of national law enforcement operating in an increasingly inter-connected world.

BIBLIOGRAPHY

Books

Adler, M., & Himma, K. E. (2009) *The rule of recognition and the US Constitution*. New York: Oxford University Press.

Aid, M. M., & Wiebes, C. (2013) *Secrets of Signals Intelligence During the Cold War: From Cold War to Globalization*. Abingdon: Routledge.

Alibek, K., & Handelman, S. (1999) *Biohazard: The chilling true story of the largest covert biological weapons in the world-Told from the inside by the man who ran it.* New York: Random House. Available online at https://www.nlm.nih.gov/nichsr/esmallpox/biohazard_alibek.pdf, Accessed 12/05/2015.

Almond, G., & Verba, S. (1963) *The civic culture: political attitudes and democracy in five countries*. Princeton: Princeton University Press.

Andress, J., & Winterfeld S. (2011) *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Boston: Syngress.

Arnas, N. (2009) *Fighting chance: global trends and shocks in the national security environment*. Washington, D.C.: Potomac Books, Inc.

Bartlett, J. (2015) *The Dark Net: Inside the Digital Underworld*. New York: Melville House Publishing.

Bauer, F. L. (2002) *Decrypted secrets: methods and maxims of cryptology*. Springer Science & Business Media.

Berger, T. U. (1998) *Cultures of Antimilitarism: national security in Germany and Japan*. Baltimore: JHU Press.

Bergström, M., Mitsilegas, V., Konstadinides, T. (2015) *Research Handbook on EU Criminal Law*. Edward Elgar Publishing.

Berkowitz, B. D., & Goodman, A. E. (1991) *Strategic intelligence for American national security*. Princeton: Princeton University Press.

Bidgoli, H. (2004) *The internet encyclopedia* (Vol. 3) Hoboken: John Wiley & Sons.

Biehl, H., & Giegerich, B. (2013) *Strategic Cultures in Europe*: *Security and Defence Policies Across the Continent*. Potsdam: Springer VS.

Biscop, S., & Andersson, J. J. (Eds.) (2007) *The EU and the European security strategy: forging a global Europe*. Abingdon: Routledge.

Bohman, J. (1993) *New philosophy of social science: Problems of indeterminacy.* Cambridge, MA: MIT Press.

Booth, K. (2014) *Strategy and Ethnocentrism* (Routledge Revivals) Abingdon: Routledge. First published in 1979.

Booth, K., & Trood, R. B. (1999) *Strategic cultures in the Asia-Pacific region*. New York: St. Martin's Press.

Brenner, S. W. (2010) *Cybercrime: criminal threats from cyberspace*. Santa Barbara, CA: Praeger.

Casey, E. (2011) *Digital evidence and computer crime: Forensic science, computers, and the internet*. London: Academic press.

Cavelty, D. M. (2008) *Cyber-Security and Threat Politics: US efforts to secure the information age*. Abingdon: Routledge.

Choucri, N. (2012) *Cyberpolitics in international relations*. Cambridge: MIT Press.

Christou, G. (2015) *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Basingstoke: Palgrave Macmillan.

Claassens, L. J., & Spronk, K. (2013) *Fragile dignity: intercontextual conversations on scriptures, family, and violence*. Atlanta: Society of Biblical Literature.

Clancy, T. K. (2011) *Cyber Crime and Digital Evidence: Materials and Cases*. New Providence: LexisNexis.

Clough, J. (2010) *Principles of Cybercrime*. Cambridge: Cambridge University Press.

Clough, P. & Nutbrown, C. (2012) *A student's guide to methodology*. London: Sage.

Cooper Jr, J. M. (2009) *Woodrow Wilson*: A biography. New York: Alfred A. Knopf.

Coupland, P. (2006) *Britannia, Europa and Christendom: British Christians and European Integration*. London: Palgrave Macmillan.

Creeber, G., & Martin, R. (2008) *Digital Culture: Understanding New Media: Understanding New Media*. New York: McGraw-Hill Education (UK)

Deflem, M. (2010) *The Policing of Terrorism* (London: Routledge).

Denning, P. J. (1991) *Computers under attack: intruders, worms, and Viruses*. New York, N.Y.: ACM Press

Denscombe, M. (2007) *The Good Research Guide: For Small-scale Social Research*. Buckingham: Open University Press.

Denzin, N. K., & Lincoln, Y. S. (2011) *The SAGE handbook of qualitative research*. London: Sage.

Diedrichs, U., Reiners, W., & Wessels, W. (Eds.) (2011) *The dynamics of change in EU governance*. Cheltenham: Edward Elgar Publishing.

Dover, R., & Goodman (Eds.) (2009) *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence*. New York: Columbia University Press.

Dover, R., & Goodman (Eds.) (2011) *Learning From the Secret Past: Cases in British Intelligence History*. Washington DC: Georgetown University Press.

Drent, M., and Zandee, D. (2010) *Breaking Pillars: Towards a Civil–Military Security Approach for the European Union.* The Hague: Netherlands Institute of International Relations Clingendael.

Flammini, F., Setola, R., & Franceschetti, G. (2013) *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues*. London: CRC Press.

Forsberg, T., & Herd, G. P. (2006) *Divided West: European Security and the Transatlantic Relationship*. London: RIIA and Blackwells Publishing Ltd.

Friedman, L. (1994) *Crime and punishment in American history*. New York: Basic Books.

Geertz, C. (1973) *The interpretation of cultures: Selected essays* (Vol. 5019). New York: Basic books.

Gibson, W. (1995) *Neuromancer*. 1984. New York: Ace.

Goldsmith, J. L., & Wu, T. (2006) *Who controls the Internet? Illusions of a borderless world.* New York: Oxford University Press.

Gomm, R. (2008) *Social research methodology: A critical introduction*. New York: Palgrave Macmillan.

Gray, C. H. (2005) *Peace, war and computers*. London: Routledge.

Greenleaf, G. (2014) *Asian Data Privacy Laws: Trade & Human Rights Perspectives*. Oxford University Press.

Hampton, M. (2013) *A Thorn in Transatlantic Relations: American and European Perceptions of Threat and Security*. New York: Palgrave Macmillan

Hanhimäki, J., Soutou, G. H., & Germond, B. (Eds.) (2010) *The Routledge handbook of transatlantic security*. Abingdon: Routledge.

Harris, B. (2008) *America, technology and strategic culture: a Clausewitzian assessment*. London: Routledge.

Harris, S. (2014) *@ War: The Rise of the Military-Internet Complex*. Boston, New York: Houghton Mifflin Harcourt.

Hartz, L. (1991) *The Liberal Tradition in America*. New York: Mariner Books.

Healey, J. (Ed.) (2013) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Washington DC: Cyber Conflict Studies Association.

Herlin-Karnell, E. (2012) *The constitutional dimension of European criminal law*. Oxford: Hart Publishing Ltd.

Herrmann, D. S. (2001) *A practical guide to security engineering and information assurance*. CRC Press.

Hinsley, S. F. & Stripp, A. (2001) *Codebreakers: the inside story of Bletchley Park*. Oxford: Oxford University Press.

Hixson, W. L. (2008) *The myth of American diplomacy: National identity and US foreign policy*. New Haven: Yale University Press.

Hope, I. C. (2015) *A Scientific Way of War: Antebellum Military Science, West Point, and the Origins of American Military Thought*. University of Nebraska Press.

Howorth, J. (2007) *Security and Defence Policy in the European Union.* Basingstoke: Palgrave Macmillan.

Hudson, V. M. (Ed.) (1997) *Culture & foreign policy*. Boulder: L. Rienner Publishers.

Jarvis, L., MacDonald, S., & Chen, T. M. (2015) *Terrorism Online: Politics, Law and Technology*. Abingdon: Routledge.

Johnson, C. (2007) *The sorrows of empire: Militarism, secrecy, and the end of the republic*. New York: Macmillan.

Jordan, T. (1999) *Cyberpower: The culture and politics of cyberspace and the Internet*. London: Routledge.

Kagan, R. (2003) *Of Paradise and Power: America and Europe in the New World Order*. New York: Knopf.

Kartchner, K. M., Johnson, J. L., & Larsen, J. A. (2009) *Strategic culture and weapons of mass destruction: culturally based insights into comparative national security policymaking*. New York: Palgrave Macmillan.

Katzenstein, P.J. (1996) *The Culture of National Security: Norms and Identity in World Politics.* New York: Columbia University Press.

Kaunert, C., & Léonard, S. (Eds.). (2013) *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe*. Hampshire: Palgrave Macmillan.

Kaunert, C., Léonard, S., & Pawlak, P. (Eds.) (2012) *European homeland security: a European strategy in the making?* Abingdon: Routledge.

Keohane, R. O. (1984) *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.

Kirby, D. (2003) *Religion and the Cold War*. New York: Palgrave Macmillan UK.

Kirchner, E. & Sperling, J. (2007) *Global security governance: competing perceptions of security in the 21st century*. London: Routledge.

Kirchner, E. J., & Sperling, J. (2010) *National security cultures: patterns of global governance*. London: Routledge.

Kiyuna, A., & Conyers, L. (2015) *Cyber warfare sourcebook*. Lulu.com

Koblentz, G. D. (2009) *Living weapons: Biological warfare and international security*. Ithaca and London: Cornell University Press.

Kohut A., & Stokes, B. (2006) *America against the World: How We Are Different and Why We Are Disliked.* New York: Times Books.

Krasner, S. D. (1983) *International regimes*. Cambridge: Cornell University Press.

Krebs, B. (2014) *Spam nation: The inside story of organized cybercrime-from global epidemic to your front door*. Naperville: Sourcebooks, Inc.

Lagadec, E. (2012) *Transatlantic relations in the 21st century: Europe, America and the rise of the rest*. Abingdon: Routledge.

Lane, J. E., & Ersson, S. (2005) *Culture and politics: a comparative approach*. Aldershot: Ashgate.

Larivé, M. H. (2014) *Debating European Security and Defense Policy: Understanding the Complexity*. Surrey: Ashgate Publishing, Ltd.

Lemieux, Frédéric (2015) *Current and emerging trends in cyber operations: Policy, strategy and practice*. Basingstoke: Palgrave Macmillan.

Lindberg, T. (Ed.). (2005) *Beyond paradise and power: Europe, America, and the future of a troubled partnership*. London: Routledge.

Litke, J. B. (2013) *Twilight of the Republic: Empire and Exceptionalism in the American Political Tradition*. Lexington: University Press of Kentucky.

Lloyd, I. (2014) *Information technology law*. Oxford: Oxford University Press.

Longhurst, K. (2004) *Germany and the use of force: The evolution of German security policy 1990-2003*. Manchester University Press.

Margetts, H. (2012) *Information technology in government: Britain and America*. London: Routledge.

Marsh, S., & Rees, W. (2012) *European Union security: from Cold War to terror war*. London: Routledge.

Mayer, P., & Rittberger, V. (1993) *Regime theory and international relations*. Oxford: Clarendon Press.

McDougall, W. (2005) *Freedom Just Around the Corner: A New American History, 1585–1828.* New York: Harper Perennial.

McKnight, G. (1973) *Computer crime.* London: Michael Joseph.

Merlingen, M. (2012) *European Security and Defense Policy: What It Is, How It Works, Why It Matters*. Boulder, CO: Lynne Rienner.

Meyer, C. O. (2006) *The quest for a European strategic culture: changing norms on security and defense in the European Union*. Basingstoke: Palgrave Macmillan.

Miles, M. B., & Huberman, A. M. (1994) *Qualitative data analysis: An expanded sourcebook*. London: Sage.

Miller, T., Birch, M., Mauthner, M., & Jessop, J. (Eds.) (2012) *Ethics in qualitative research*. London: Sage.

Milner, E. R. (2003) *The Lives and Times of Bonnie & Clyde*. Carbondale: SIU Press.

Moran, C. (2013) *Classified: Secrecy and the State in Modern Britain*. Cambridge: Cambridge University Press.

Mueller, M. L. (2010) *Networks and states: The global politics of Internet governance*. Cambridge: The MIT Press.

Nadelmann, E. A. (2010) *Cops across borders: The internationalization of US criminal law enforcement*. University Park: Pennsylvania State University Press.

Nedergaard, P. (2007) *European Union administration: legitimacy and efficiency*. Leiden /Boston: Martinus Nijhoff Publishers.

Nye, J. S. (2011) *The future of power*. New York: Public Affairs.

Ostrom, E. (2015) *Governing the commons: The evolution of institutions for collective action*. Cambridge: Cambridge University Press.

Peters, B. G., & Pierre, J. (Eds.) (2004) *The Politicization of the Civil Service in Comparative Perspective: A Quest for Control*. London/ New York: Routledge.

Pinkowski, J. (2008) *Homeland Security Handbook.* New York: CRC Press, Taylor and Francis Group.

Piris, J. C. (2010) *The Lisbon Treaty: a legal and political analysis*. Cambridge: Cambridge University Press.

Pollicino, O. and Romeo, G. (Eds.), (2016) *The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe*. Abingdon, Oxon; New York, NY: Routledge.

Porter, B. (1989) *Plots and Paranoia: A History of Political Espionage in Britain, 1790-1900*. London: Unwin Hyman.

Powell, W.W. & DiMaggio, P. (1991) *The New Institutionalism in Organizational Analysis.* Chicago, IL: University of Chicago Press.

Putnam R. & Campbell, D. E. (2010) *American Grace: How Religion Divides and Unites Us.* New York: Simon and Schuster.

Rees, W. (2006) *Transatlantic Counter Terrorism Cooperation: The New Imperative*. London: Routledge.

Rees, W. (2011) *The US-EU Security Relationship: The Tensions between a European and a Global Agenda*. Basingstoke: Palgrave Macmillan.

Reiter, D. (1996) *Crucible of beliefs: learning, alliances and world wars*. Ithaca, NY: Cornell University Press.

Reyes, A., Brittson, R., O'Shea, K., & Steele, J. (2011) *Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors*. Massachusetts: Syngress.

Rid, T. (2013) *Cyber war will not take place*. New York: Oxford University Press.

Ritchie, J., Lewis, J., Nicholls, C. M., & Ormston, R. (Eds.). (2013) *Qualitative research practice: A guide for social science students and researchers*. London: Sage.

Rosen, S. P. (1996) *Societies and military power: India and its armies*. Ithaca: Cornell University Press.

Sanders, R. (1999) *The executive decision making process: identifying problems and assessing outcomes*. Greenwood Publishing Group.

Santanam, R. (Ed.) (2010) *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives: Applications and Perspectives*. IGI Global.

Schell, B. H., & Martin, C. (2004) *Cybercrime: A reference handbook*. Santa Barbara, Calif: ABC-CLIO.

Schmidt, P., & Zyla, B. (2013) *European Security Policy and Strategic Culture*. Abingdon: Routledge.

Schmidt, S. W., Shelley, M. C., & Bardes, B. A. (2014) *American Government and Politics Today, 2013-2014 Edition*. Wadsworth: Cengage Learning.

Schmitt, M. N. (ed.) (2013) *Tallinn manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press.

Schneier, B. (2011) *Secrets and lies: digital security in a networked world*. Indianapolis: John Wiley & Sons.

Schönbohm, A. (2012) *Germany's Security: Cyber Crime and Cyber War*. Münster: Edition Octopus.

Sheehan, J. J. (2008) *Where have all the Soldiers Gone? The Transformation of Modern Europe.* New York: Mariner Books.

Shenhav, Y. A. (2002) *Manufacturing rationality: The engineering foundations of the managerial revolution*. Oxford and New York: Oxford University Press.

Shinder, D. L., & Cross, M. (2008) *Scene of the Cybercrime*. (2nd ed.) Burlington, MA: Syngress.

Shore, C. (2001) *Building Europe: The cultural politics of European integration*. Abingdon: Routledge.

Shore, Peter (2000) *Separate Ways*. London: Duckworth.

Silverman, D. (2013) *Doing qualitative research: A practical handbook*. London: SAGE Publications Limited.

Singer, P. W., & Friedman, A. (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know*. London: Oxford University Press.

Smith, M. E. (2004) *Europe's foreign and security policy: the institutionalization of cooperation*. Cambridge: Cambridge University Press.

Snyder, J. L. (1977) *The Soviet Strategic Culture: Implications for Limited Nuclear Operations*. Santa Monica: Rand Corp.

Sondhaus, L. (2006) *Strategic culture and ways of war*. Abingdon Oxon: Routledge.

Sottiaux, S. (2008) *Terrorism and the Limitation of Rights: The ECHR and the US Constitution*. Oxford and Portland: Hart Publishing.

Steinbock, D. (2003) *Wireless horizon: Strategy and competition in the worldwide mobile marketplace*. Washington, D.C.: Amacom.

Sterling, B. (1993) *The Hacker Crackdown.* McLean, Virginia: Indy Publish

Sterling, C. H. (Ed.). (2008) *Military communications: from ancient times to the 21st century*. Oxford: Abc-clio, Inc.

Strazzella, J. A. (1998) *The federalization of criminal law*. Task Force on the Federalization of Criminal Law, Washington, D.C.: American Bar Association, Criminal Justice Section.

Summers, S., Schwarzenegger, C., Ege, G., & Young, F. (2014) *The emergence of EU criminal law: cyber crime and the regulation of the information society*. Oxford: Bloomsbury Publishing.

Sutton, R. P. (2002) *Federalism*. Greenwood Publishing Group.

Swan, Sean (2012) *On the Cyber*. Lulu

Toje, A. (2008) *America, the EU and strategic culture: renegotiating the transatlantic bargain*. London: Routledge.

Tzu, S. (1983) *The art of war*. (Ed.) James Clavell. London: Hodder and Stoughton.

Wall, D. (2001) *Crime and the Internet*. London: Routledge.

Wall, D. (2003) *Cyberspace crime*. Aldershot: Ashgate Publishing Company.

Weigley, R. F. (1977) *The American way of war: a history of United States military strategy and policy*. Bloomington: Indiana University Press.

White, L. D. (1954) *The Jacksonians: A study in administrative history*. New York: Macmillan.

Yannakogeorgos, P. A., & Lowther, A. B. (Eds.) (2013) *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. London: Taylor and Francis Group.

Zittrain, J. (2008) *The future of the internet - and how to stop it*. New Haven: Yale University Press.

Conferences

Conference papers-presented:

Nagyfejeo, E. (2013) 'How feasible is EU-U.S. collaboration in countering cyberterrorism?' in Swansea University's Cyberterrorism Project's Multidisciplinary Conference on Cyberterrorism, Birmingham, 12 April 2013

Nagyfejeo, E. (2015) 'The EU-U.S. cyber dialogue between security and freedom' in The European Union: a Cybersecurity Actor? (Trans)national agencies, discourses and practices; Two-day workshop on European Cybersecurity sponsored by the French Ministry of Defence Strategic Research Institute (IRSEM) and the Manchester Jean Monnet Centre of Excellence (MJMCE), University of Manchester, 22-23 January 2015

Nagyfejeo, E. (2016) 'EU – U.S. cyber diplomacy' at Europol's EC3 Academic Advisory Network (EC3 AAN), Europol, The Hague, 6-7 April 2016.

Participated:

- 17-18th May 2013: Intelligence in the Cyber Environment - organised by Brunel Centre for Intelligence & Security Studies
- 6th June 2013: 2nd Microsoft EU Cyber Security Forum, Brussels
- 10-11th June 2013: Cyber Security: Balancing risks, responsibilities and returns - organised by Chatham House, London
- June 20 2013: EU Cyber Security cooperation - organised by Royal Military Academy, Brussels
- 25th September 2013: Cyber Security Roundtable discussion - hosted by Andreas Schwab, MEP, Brussels, EU Parliament
- 12th November 2013: Huawei - Cyber Security Whitepaper (Brussels)
- 14th November 2013: SDA – Cyber Security Professional Wanted (Brussels)
- 26th November 2013 – Tackling cybercrime – hosted by European Voice (Brussels)
- 28th February 2014 - High Level Cyber security Conference hosted by DG Connect

- 4-5th March 2014 - 5th Annual Internet of Things European Summit (Brussels)
- 20-21st March 2014 - European Internet Governance and Beyond (EU Parliament, Brussels)
- 25th March 2014 - The 2nd Annual European Cyber Security Conference (Brussels)
- 8th April 2014 - The 3rd Annual European Cloud Computing Conference (Brussels)
- 22-24th September 2014 - Cyber Intelligence Europe Conference, Brussels
- 19-20th May 2014 – Cyber Security: Building Resilience, Reducing Risks - organised by Chatham House, London
- 4-5th February 2015 - ICSS 2015, The International Cyber Security Strategy Congress: "Cyber Security and Forensic Readiness, Leuven, Belgium
- 13-15th April 2015 – Global Conference on Cyberspace, The Hague
- 15th April 2015 - LEAP2015 side conference on cybercrime, Europol, The Hague
- All the Cyber Risk Wednesday events organised by the Atlantic Council each month (20th May, 17th June, 29th July, 19th August 2015)
- 18th May 2015 - Surveillance and Future of the Internet held at George Washington University
- 20-21st May 2015 - Third Annual Cybersecurity Law Institute held at Georgetown University Law Center
- 2-5th June 2015 - U.S. Department of Homeland Security, Supply Software and Supply Chain Assurance Forum
- 8-10th June 2015 - Gartner Security and Risk Management Summit
- 23rd June 2015 - Georgetown University Law School, Internet of Things cyber event
- 24th June 2015 - Newseum, Managing the Risks of Digital Frontier
- 9th July 2015- Cyber security Breakfast event organised at University Club
- 26th August 2015 - Cyber Security Sessions organised by the Digital Government Institute
- 4th November 2015 - EU Cybercrime Task Force (EUCTF) at Europol

Interviews

Interview (2014a) conducted with a former MEP (Liberal Democrat) from the EU Parliament, Brussels, April.

Interview (2014b) conducted with a former MEP (European Conservatives and Reformists Group) from the EU Parliament, Brussels, April.

Interview (2014c) conducted with a NATO official, Brussels, May.

Interview (2014d) conducted with an EEAS cyber official, Brussels, September.

Interview (2014e) conducted with a Counsellor from the Permanent Delegation of Hungary to NATO, Brussels, May.

Interview (2014f) conducted with an official from DG HOME, Brussels, June.

Interview (2014g) conducted with the International Outreach Coordinator for Cyber Issues of the Ministry of Foreign Affairs and Trade – Hungary, Budapest, September.

Interview (2014h) conducted with a Korean Police Officer, Oxford, December.

Interview (2014i) conducted with an official from DG CONNECT, Brussels, February.

Interview (2014j) conducted with a cyber policy advisor to the EPP group, Brussels, April.

Interview (2015a) conducted with a Programme Manager Cyber Defence from the European Defence Agency, Leuven, Belgium, February.

Interview (2015b) conducted with an officer from ENISA, Europol, EC3, The Hague, November.

Interview (2015c) conducted with a senior strategic analyst from Europol, EC3, The Hague, November.

Interview (2015d) conducted with a senior cyber officer from Europol, EC3, The Hague, December.

Interview (2015e) conducted with a counsellor on digital economy and cyber from the Delegation of the European Union to the United States, Washington, DC, August.

Interview (2015f) conducted with an ICE-HSI Special Agent, Europol, The Hague, December.

Interview (2015g) conducted with an analyst at the Case Analysis Unit from Eurojust, Europol, The Hague, December.

Interview (2015h) conducted with a senior official from EC3 Prevention and Outreach, Europol, The Hague, November.

Interview (2015i) conducted with a senior official from EC3 Strategy and Development, Europol, The Hague, December.

Interview (2015j) conducted with the Director of Government Relations and Public Affairs from Symantec, Europol, The Hague, November.

Interview (2015k) conducted with a J-CAT cyber liaison officer from EC3, Europol, The Hague, December.

Interview (2015l) conducted with a former HM government officer, Washington, DC, June.

Interview (2015m) conducted with a Europol senior representative from the Delegation of the European Union to the United States, Washington, DC, July.

Interview (2015n) conducted with a former senior Information Assurance Representative of the NSA, Washington, DC, July.

Interview (2015o) conducted with an official from the U.S. DSS, Europol, The Hague, December.

Interview (2015p) conducted with an official from the US–FDA, Europol, The Hague, December.

Interview (2015q) conducted with an official from the U.S. CERT, National Cybersecurity & Communications Integration Center, DHS, Washington, DC, May.

Interview (2015r) conducted with a consultant from Hatha Systems, Washington, DC, May.

Interview (2015s) conducted with an official from the Coalition Law Division in the Directorate of Operations and International Law, HQ USAF, Pentagon, Washington, DC, May.

Interview (2015t) conducted with Professor Frederic Lemieux from George Washington University, Washington, DC, July.

Interview (2015u) conducted with a former DOJ cybercrime prosecutor, Washington, DC, May.

Interview (2015v) conducted with a senior advisor for Information Security, NIST, Washington, DC, May.

Interview (2015w) conducted with a former NSA and CIA Director, Washington, DC, August.

Interview (2016a) conducted with an US Cybercrime Liaison Prosecutor from the US DOJ/CCIPS, Europol, The Hague, February.

Interview (2016b) conducted with an FBI Cyber Liaison to Europol's Cyber Crime Center, Europol, The Hague, February.

Interview (2016c) conducted with an agent from the United States Secret Service, Europol, The Hague, March.

Interview (2016d) conducted with supervisory special agent from the FBI, Europol, The Hague, March.

Interview (2016e) conducted with a cybercrime prosecutor from Eurojust, Europol, The Hague, February.

Journal articles and chapters in books

Adams, J. A. M. (1996) 'Controlling cyberspace: applying the computer fraud and abuse act to the Internet', *Santa Clara Computer & High Tech. LJ*, 12:403.

Akcadag, Emine (2012) 'The growing cyber-threat: What role for the Transatlantic Alliance?', *Atlantic Voices*, 2/5: 1-10.

Aldrich, R. (2009) 'US-European Intelligence Co-operation on Counter-Terrorism: Low Politics and Compulsion', *The British Journal of Politics and International Relations*, 11/1: 122-139.

Aldrich, R. & Herrington, L. (2013) 'The future of cyber-resilience in an age of global complexity', *Politics*, 33/4: 299-310.

Aldrich, R. & Rees, W. (2005) 'Contending cultures of counter-terrorism: transatlantic divergence or convergence?' *International Affairs*, 81/5: 905-923.

Arquilla J. and Ronfeldt, D. (1993) 'Cyberwar is Coming!', *Comparative Strategy*, 12/2: 141–65.

Bailes, A. (1999) 'European Defence: What are the Convergence Criteria?' *RUSI Journal*, 144/3: 60–65.

Baker, G. D. (1993) Trespassers Will Be Prosecuted: Computer Crime in the 1990s, 12 Computer LJ 61, *The John Marshall Journal of Information Technology & Privacy Law*, 12/1: 4. Available online at: http://repository.jmls.edu/cgi/viewcontent.cgi?article=1371&context=jitpl, Accessed 14/06/2013.

Bendiek A. (2014) 'Tests of Partnership: Transatlantic cooperation in cyber security, Internet governance and data protection', Transatlantic Academy Paper Series, No. 1, 2013–14 paper series: 1–33.

Bendrath, R. (2001) 'The cyberwar debate: Perception and politics in US critical infrastructure protection' in *Information & Security: An International Journal*, 7: 80–103.

Biava, A., Drent, M., & Herd, G. P. (2011) 'Characterizing the European Union's Strategic Culture: An Analytical Framework', *JCMS: journal of common market studies*, 49/6: 1227-1248.

Bignami, F. (2007) 'European versus American liberty: a comparative privacy analysis of anti-terrorism data-mining', *Boston College Law Review*, *48*: 609.

Biscop, S., & Coelmont, J. (2011) Europe deploys towards a civil-military strategy for CSDP. *Egmont Paper*, 49. Brussels: Royal Institute of International Relations.

Biscop, S., & Norheim-Martinsen, P. M. (2011) 'CSDP: The Strategic Perspective', In Kurowska, X., & Breuer, F. (Eds.) *Explaining the EU's Common Security and Defence Policy: Theory in Action.* Basingstoke: Palgrave Macmillan UK.

Booth, K. (1990) 'The concept of strategic culture affirmed', in Jacobsen, C. G. Ed. *Strategic Power: USA/USSR*. London: Palgrave Macmillan UK.

Brenner, S. B. (2013) 'Cyber-threats and the Limits of Bureaucratic Control', *Minnesota Journal of Law, Science & Technology*, 14/1: 137-258. Available

online at: http://scholarship.law.umn.edu/mjlst/vol14/iss1/6, Accessed 26/12/2015.

Brickey, K. F. (1995) 'Criminal mischief: the federalization of American criminal law', *Hastings Law Journal*, 46: 1135- 1174.

Bryman, A. (2006) 'Integrating quantitative and qualitative research: how is it done?', *Qualitative research*, 6/1: 97-113.

Bures, O. (2006) 'EU counterterrorism policy: a paper tiger?', *Terrorism and political violence*, 18/1: 57-78.

Bures, O. (2013) 'Europol's Counter-terrorism Role: A Chicken-Egg Dilemma' in Kaunert Christian and Léonard S. (Eds) *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe*. Hampshire: Palgrave Macmillan.

Byrne, A. (2012) 'Building the Transatlantic Area of Freedom, Security and Justice. The case of the Passenger Name Record Agreements', *IAI working Papers*, 12/6: 1-18.

Camillo, F., & Miranda, V. (2011) '*Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward*', *Istituto Affari Internazionali*, 11/26: 1-23. Available online at http://www.iai.it/pdf/dociai/iaiwp1126.pdf, Accessed 10/10/2012.

Cavelty, D. M. (2007) 'Critical information infrastructure: vulnerabilities, threats and responses', UNIDIR *Disarmament Forum: ICTs and International Security*, 3: 15-22.

Cavelty, D. M. (2012) 'Cyber security', in: Allan Collins (ed.) *Contemporary Security Studies*. Oxford University Press.

Checkel, J. T. (2001) 'Why comply? Social learning and European identity change', *International organization*, *55*/03: 553-588.

Choong, W. (2015) 'Defence and Japan's Constitutional Debate', *Survival*, 57/2: 173-192.

Christou, G. & Gomez, R. (2004) 'Foreign Economic Policy: The EU in the Mediterranean', In Carlsnaes, W., Sjursen, H., & White, B. (Eds.), *Contemporary European foreign policy*. London: Sage.

Clancy, T. K. (2009) 'What Does the Fourth Amendment Protect: Property, Privacy, or Security', *Wake Forest Law Review*, *33*: 307. Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1565773, Accessed 04/11/2013.

Clinton, J. D., Lewis, D. E., & Selin, J. L. (2014) 'Influencing the bureaucracy: The irony of congressional oversight', *American Journal of Political Science*, 58/2: 387-401.

Cooper, D. R., & Schindler, P. S. (2006) 'Business research methods: Empirical investigation', *Journal of service research*, 1/2: 108-28.

Cornish, P. (2013) 'United Kingdom', in Biehl, H., & Giegerich, B. (2013) *Strategic Cultures in Europe*: *Security and Defence Policies Across the Continent*. Potsdam: Springer VS.

Cornish, P., & Edwards, G. (2005) 'The strategic culture of the European Union: a progress report', *International affairs*, 81/4: 801-820.

Crosston, M. D. (2011) 'World Gone Cyber MAD', *Strategic Studies Quarterly*,*100*. Available online at http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf, Accessed 29/10/2012.

Dahle, M. H. (2012) 'The growing cyber-threat: What role for the Transatlantic Alliance?', *Atlantic Voices*, 2/5: 1-10.

Dalgaard-Nielsen, A. (2005) 'The test of strategic culture: Germany, pacifism and pre-emptive strikes', *Security Dialogue*, 36/3: 339-359.

De Goede, M. (2008) 'The Politics of Preemption and the War on Terror in Europe', *European Journal of International Relations*, 14/1: 161–85.

De Vries, G. (2005) 'The European Union's Role in the Fight Against Terrorism', *Irish Studies in International Affairs*, 16: 3–9.

De Vries, G. (2005) 'Towards a European area of freedom, security and justice?', *Challenge Europe, Issue 14, European Policy Centre website*, 16 September.

Deflem, M. (2006) 'Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective', *Justice Quarterly*, 23/3: 336–359.

Deibert, R. (2012) Growing Dark Side of Cyberspace (... and What to Do about It). *Penn St. JL & Int'l Aff.*, 1/260.

Deibert, R. J., & Crete-Nishihata, M. (2012) 'Global Governance and the Spread of Cyberspace Controls', *Global Governance: A Review of Multilateralism and International Organizations*, 18/3: 339-361.

Deibert, R. & Rohozinski R. (2010) 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology,* 4/1: 15-32.

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

Diez, T. and Manners, I. (2007) 'Reflecting on Normative Power Europe', In Felix Berenskoetter and Michael J. Williams (eds) *Power in World Politics*. London: Routledge.

Dover, R., (2014) 'The World's Second Oldest Profession: The Transatlantic Spying Scandal and its Aftermath', *The International Spectator*, 49/2:117-133.

Duchêne, F. (1973) 'The European Community and the Uncertainties of Interdependence', In M. Kohnstamm and W. Hager (eds) *A Nation Writ Large?: Foreign-Policy Problems before the European Community*. London: Palgrave Macmillan.

Eriksson, J. & Giacomello, G. (2006) 'The Information Revolution, Security, and International Relations', *International Political Science Review*, 27/3: 221-244.

Fahey, E. (2014) 'The EU's Cybercrime and Cyber-Security Rule-Making: Mapping the Internal and External Dimensions of EU Security', *European Journal of Risk Regulation*, 1:46-61.

Fried, Charles (1968) Privacy, *Yale Journal*, 77/3: 475- 493.

Geertz, C. (1973) 'Thick description: Toward an interpretive theory of culture', In *The interpretation of cultures: Selected essays*. New York: Basic Books.

George, Alexander L. (1997) 'Knowledge for Statecraft: The Challenge for Political Science and History', *International Security*, 22/1: 44–52.

Goldstein, W. (1993) 'Europe after Maastricht', *Foreign Affairs*, 117-132.

Grace Davie (1999) 'Europe: The Exception that Proves the Rule?', in Berger, *The Desecularization of the World: Resurgent religion and world politics* (pp. 65–84) Grand Rapids, Mich: Wm. B. Eerdmans Publishing Co.

Gray, C. S. (1981) National style in strategy: The American example. *International Security*, *6*/2: 21-47.

Gray, C. S. (1999) 'Strategic culture as context: the first generation of theory strikes back', *Review of international studies*, *25*/01: 49-69.

Gray, C. S. (2006) 'Out of the Wilderness: Prime Time for Strategic Culture', *Comparative Strategy*, 26/1: 1-20.

Griffith, D. S. (1990) 'Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem' *Vanderbilt Law Review*, 43/2: 453-490.

Haglund, D. G. (2011) 'Let's Call the Whole Thing Off'? Security Culture as Strategic Culture. *Contemporary Security Policy*, 32/3: 494-516.

Haine, J. Y. (2011) The Failure of a European Strategic Culture–EUFOR CHAD: The Last of its Kind?, *Contemporary security policy*, 32/3: 582-603.

Harnisch, S. and Maull, H. (2001) 'Introduction', in Hans Maull, ed., *Germany as a Civilian Power?,* Manchester: Manchester University Press.

Heisbourg, F. (2004) 'The "European Security Strategy" is not a security strategy', In Everts, S., Freedman, L., Grant, C., Heisbourg, F., Keohane, D., & O'Hanlon, M. (Eds.), *A European way of war*. London: Centre for European Reform.

Hillebrand, C. (2013) 'Guarding EU-wide counter-terrorism policing: the struggle for sound parliamentary scrutiny of Europol', In Kaunert Christian and Léonard S. (eds) *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe*. Hampshire: Palgrave Macmillan.

Hoffman, S. (1993) 'Goodbye to a United Europe', *New York Review of Books*, 41/10: 27-31.

Howorth, J. (2002) 'The CESDP and the Forging of a European Security Culture'. *Politique Europeenne*, 8: 88–108.

Hyde-Price, A. (2004) 'European Security, Strategic Culture and the Use of Force', *European Security*, 13/4: 323–43.

Jensen, E. T. (2011) 'President Obama and the Changing Cyber Paradigm' in *William Mitchell Law Review*, 37: 5049.

Johnston, A. I. (1995) 'Thinking about strategic culture', *International security*, *19*/4: 32-64.

Johnston, A. I. (1996) 'Cultural realism and strategy in Maoist China', *The Culture of national Security: norms and identity in world Politics*, 216-68.

Junk and Daase (2013) 'Germany', in Biehl, H., & Giegerich, B. (2013) *Strategic Cultures in Europe*: *Security and Defence Policies Across the Continent*. Potsdam: Springer VS.

Kaelberer, M. (2004) The euro and European identity: symbols, power and the politics of European monetary union. *Review of International Studies*, *30*/02:161-178.

Kamara, H. M. (2015) 'The Influence of US Strategic Culture on Innovation and Adaptation in the US Army', *Journal of Strategic Security*, *8*/4: 79-91.

Kammel, A. H. (2011) 'Putting ideas into action: EU civilian crisis management in the Western Balkans', *Contemporary Security Policy*, 32/3: 625-643.

Kartchner, K. M. (2009) 'Strategic culture and WMD decision making', In *Strategic Culture and Weapons of Mass Destruction* (pp. 55-67). Palgrave Macmillan US.

Kier, E. (1995) 'Culture and military doctrine: France between the wars', *International Security*, 19/4: 65-93.

Klein, B. S. (1988) 'Hegemony and strategic culture: American power projection and alliance defence politics', *Review of International Studies*, 14/02: 133-148.

Knake, R. K. (2010) *Internet governance in an age of cyber insecurity* (No. 56). Council on Foreign Relations.

Koblentz, G. D., & Mazanec, B. M. (2013) 'Viral Warfare: The Security Implications of Cyber and Biological Weapons', *Comparative Strategy*, 32/5:418-434.

Kurland, A. H. (1996) 'First Principles of American Federalism and the Nature of Federal Criminal Jurisdiction', *Emory Law Journal*, 45/1-94.

Lantis, J. S. (2002) 'Strategic culture and national security policy', *International studies review*, 4/3: 87-113.

Legro, J. W. (1994) 'Military culture and inadvertent escalation in World War II', *International Security*, 18/4: 108-142.

Lentzos, Filippa & Rose, Nikolas (2009) 'Governing insecurity: contingency planning, protection, resilience**',** *Economy and society*, 38/2230-254.

Levy, D. (2006) 'Qualitative methodology and grounded theory in property research', *Pacific Rim Property Research Journal*, 12/4: 369-388.

Levy, M. A., Young, O. R., & Zürn, M. (1995) 'The study of international regimes', *European Journal of International Relations*, 1/3: 267-330.

Libicki, M. C. (2009) 'Military Cyberpower', In Kramer, F. D., Starr, S. H., & Wentz, L. K. (Eds.), *Cyberpower and national security*. Dulles, Virginia: Potomac Books, Inc.

Libicki, M. C. (2012) 'Cyberspace is not a warfighting domain', *ISJLP*, *8*/ 321.

Lindsay, J. R. (2015) 'The impact of China on cybersecurity: fiction and friction', *International Security*, 39/3: 7-47. Available online at http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf, Accessed 12/11/2015.

Lock, E. (2010) 'Refining strategic culture: return of the second generation', *Review of International Studies*, 36/03: 685-708.

Luckham, R. (1984) 'Armament culture', *Alternatives: Global, Local, Political*, 10/1: 1-44.

Luckham, R. (1984) 'Of arms and culture', *Current Research on Peace and Violence*, 7/1: 1-64.

Lundmark, T. (2000) 'Free Speech Meets Free Enterprise in the United States and Germany', *Ind. Int'l & Comp. L. Rev.*, 11: 289.

Mailath, G. J. (1998) 'Do people play Nash equilibrium? Lessons from evolutionary game theory', *Journal of Economic Literature*, 36/3: 1347-1374.

Mancini, G. F. (1989) 'The making of a constitution for Europe', *Common Market Law Review*, *26*/4: 595-614.

Manners, I. (2002) 'Normative Power Europe: A Contradiction in Terms?', *Journal of Common Market Studies,* 40/2: 235–258.

Manners, I. (2006) 'Normative Power Reconsidered: Beyond the Crossroads', *Journal of European Public Policy*, 13/2: 182–199.

Marrone and Di Camillo (2013) 'Italy', in Biehl, H., & Giegerich, B. (2013) *Strategic Cultures in Europe*: *Security and Defence Policies Across the Continent*. Potsdam: Springer VS.

Matlary, J.H. (2006) 'When Soft Power Turns Hard: Is an EU Strategic Culture Possible?', *Security Dialogue*, 37/1: 105-121.

Maxwell, J. (1992) 'Understanding and validity in qualitative research', *Harvard educational review*, 62/3: 279-301.

Mayer, P., Rittberger, V., & Zürn, M. (1993) Regime theory: state of the art and perspectives. *Regime Theory and International Relations, Oxford*, 391-430.

McFadyen, R. C. (2008) 'Protecting the nation's Cyber Infrastructure: Is the Department of Homeland Security Our Nation's Savior or the Albatross Around Our Neck', *I/S: Journal of Law and Policy for the Information Society*, *5*/2: 319- 379.

McStay, A. (2012) 'I consent: An analysis of the Cookie Directive and its implications for UK behavioural advertising', *New Media & Society*, 15/4: 596-611.

Mead, W. R. (2004) 'America's sticky power' in *Foreign Policy*, 141 (March): 46–53.

Merriam, S. B. (2002) 'Introduction to qualitative research', *Qualitative research in practice: Examples for discussion and analysis*, 1/ 1-17.

Meyer, C. O. (2005) 'Convergence towards a European strategic culture? A constructivist framework for explaining changing norms', *European Journal of International Relations*, 11/4: 523-549.

Miller, L. L., & Eisenstein, J. (2005) 'The federal/state criminal prosecution nexus: A case study in cooperation and discretion', *Law & Social Inquiry*, 30/2: 239-268.

Myers, R. (2008) 'Responding to the Time-Based Failures of the Criminal Law Through a Criminal Sunset Amendment', *Boston College Law Review*, 49/5.

Nagyfejeo, E. (2012) 'European cyber security challenges: why is the European Union unable to develop a joint approach to cyber security?', Master thesis, School of Politics & International Relations, University of Nottingham.

Nagyfejeo, E. (2015) 'Transatlantic collaboration in countering cyber terrorism', In L. Jarvis, S. MacDonald, T. M. Chen, (Eds.). *Terrorism online*. Abingdon, Oxon; New York, NY: Routledge.

Neumann, I. B., & Heikka, H. (2005) 'Grand Strategy, Strategic Culture, Practice The Social Roots of Nordic Defence', *Cooperation and Conflict*, 40/1: 5-23.

Newton, N. (2010) 'The use of semi-structured interviews in qualitative research: strengths and weaknesses', *Exploring qualitative methods*, 1/1: 1-11.

Nickolov, E. (2005) 'Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations' in *An International Journal*, 17: 105–19.

Norheim-Martinsen, P. M. (2011) 'EU strategic culture: When the means becomes the end', *Contemporary Security Policy*, 32/3: 517-534.

Occhipinti, J. (2013) 'Availability By Stealth? EU Information-sharing in Transatlantic Perspective', In Kaunert Christian and Léonard S. (eds) *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe*. Hampshire: Palgrave Macmillan.

Peiravi, A. (2010) Internet security - cyber crime paradox', *Journal of American Science*, 6/1: 15-24.

Pentland, C. C. (2011) 'From words to deeds: strategic culture and the European Union's Balkan military missions', *Contemporary security policy*, 32/3: 551-566.

Peter Berger (1999) 'The Desecularization of the World: A Global View,' in Peter Berger, ed., *The Desecularization of the World: Resurgent Religion and World Politics.* Washington, DC: Ethics and Public Policy Center; Grand Rapids, MI: W. B. Eerdmans Publishing.

Peters, I. (2011) 'Strategic culture and multilateralism: The interplay of the EU and the UN in conflict and crisis management', *Contemporary Security Policy*, 32/3: 644-666.

Piper, P. (2008) 'Nets of terror: Terrorist activity on the Internet', *Searcher*, 16/10: 28-38.

Pirani, P. (2014) 'Elites in Action: Change and Continuity in Strategic Culture', *Political Studies Review*.

Poore, S. (2003) 'What is the context? A reply to the Gray-Johnston debate on strategic culture', *Review of International Studies*, 29/02: 279-284.

Post, Robert C. (2001) 'Three Concepts of Privacy', *Faculty Scholarship Series*. Paper 185. Available online at http://digitalcommons.law.yale.edu/fss_papers/185, Accessed 19/04/2015.

Rasch, M. (1996) 'Criminal law and the internet', *The Internet and Business: A Lawyer's Guide to the Emerging Legal issues. Retrieved February*, *5*, 1999.

Rasmussen, M.V. (2005) 'What's the Use of It? Danish Strategic Culture and the Utility of Armed Force', *Co-operation and Conflict*, 40/1: 67–89.

Reiter, D. (1994) 'Learning, realism, and alliances', *World Politics*, 46/4: 490–526.

Rice, M., Miller, R., & Shenoi, S. (2011) 'May the US government monitor private critical infrastructure assets to combat foreign cyberspace threats?',*International Journal of Critical Infrastructure Protection*, 4/1: 3-13.

Richman, D. C. (2000) 'The changing boundaries between federal and local law enforcement', *Criminal Justice,* 2: 81-82.

Richman, Daniel C. (2005) 'The Future of Violent Crime Federalism', *Fordham Law Faculty Colloquium Papers*. Paper 11. Available online at http://lsr.nellco.org/fordham_fc/11, Accessed 19/07/2014.

Robinson, N. (2014) 'EU cyber-defence: a work in progress', *European Union Institute for Security Studies*. Available online at http://www.iss.europa.eu/uploads/media/Brief_10_Cyber_defence.pdf, Accessed 23/02/2015.

Rotter, A. J. (2002) Christians, Muslims, and Hindus: Religion and US-South Asian Relations, 1947–1954. *Diplomatic History*, 24/4: 593-613.

Russel, Charles A. (1979) 'Europe Regional Review', in *Terrorism: An International Journal*, 3/1-2: 158.

Rynning, S. (2011a) 'Realism and the common security and defence policy', *Journal of Common Market Studies*, 49/1: 23-42.

Rynning, S. (2011b) 'Strategic culture and the common security and defence policy–A classical realist assessment and critique', *Contemporary Security Policy*, 32/3: 535-550.

Schlanger, M. (2015) 'Intelligence Legalism and the National Security Agency's Civil Liberties Gap', *6 Harvard National Security Journal 112*, University of Michigan Public Law Research Paper No. 432. Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2495844, Accessed 14/02/2016.

Schmidt, P., & Zyla, B. (2011) 'European security policy: Strategic culture in operation?', *Contemporary security policy*, 32/3: 484-493.

Schwandt, T. (2007) 'Thick description', In *Qualitative inquiry: A dictionary of terms*. Thousand Oaks: CA: Sage Publications, Inc.

Smith, F.B. (1970) 'British Post Office Espionage, 1844', *Historical Studies,* 14/54: 189-203.

Smith, M. (2004a) 'Between two worlds? The European Union, the United States and world order', *International Politics*, 41/1: 95-117.

Smith, M. E. (2004b) 'Institutionalization, policy adaptation and European foreign policy cooperation', *European Journal of International Relations*, 10/1: 95-136.

Stuart-Fox, M. (2004) Southeast Asia and China: the role of history and culture in shaping future relations. *Contemporary Southeast Asia*, 116-139.

Sullivan, C. L. (2014) 'Cybersecurity and the ANZUS Treaty: The Issue of US-Australian Retaliation', *Georgetown Journal of International Affairs,* Available online at http://journal.georgetown.edu/cybersecurity-and-the-anzus-treaty-the-issue-of-u-s-australian-retaliation/, Accessed 23/06/2015.

Swidler, A. (1986) 'Culture in action: Symbols and strategies', *American sociological review*, *51*/2: 273-286.

US Congress (1988) 'Computer Security Act of 1987', *Public Law*, 100-235.

Van Ham, P. (2005) 'Europe's strategic culture and the relevance of war', *Oxford Journal on Good Governance*, 2/1: 39-44.

Vincent, D. (1991) 'The Origins of Public Secrecy in Britain', *Transactions of the Royal Historical Society,* 6/1: 229-248.

Wæver, Ole, (1998) 'The Sociology of a Not So International Discipline: American and European Developments in International Relations', *International Organization*, 52/4: 687-727.

Walsham, G. (2006) 'Doing interpretive research', *European journal of information systems*, 15/3: 320-330.

Warner, M. (2012) 'Cybersecurity: a pre-history', *Intelligence and National Security*, 27/5: 781-799.

Whitman, J. Q. (2004) 'The two western cultures of privacy: dignity versus liberty', *Yale Law Journal*, 113: 1151-1221. Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=476041, Accessed 24/05/2015.

Wilson, W., & Pestritto, R. J. (2005) 'Christ's Army', reprinted in *Woodrow Wilson: the essential political writings*. Lanham, MD: Lexington Books.

Young, O. R. (1986) 'International regimes: Toward a new theory of institutions', *World Politics*, 39/01: 104-122.

Zyla, B. (2011) 'Overlap or Opposition? EU and NATO's Strategic (Sub-) Culture', *Contemporary Security Policy*, 32/3: 667-687.

Other documents, online news articles, newspapers, speeches

Access Press Release (2015) 'French Senate ratifies international surveillance law, threatens privacy worldwide (27/10/2015)', *Access*. Available online at https://s3.amazonaws.com/access.3cdn.net/19724050a143d70961_trm6bn2o2.pdf, Accessed 11/12/2015.

ACLU and Friends of Privacy USA (2013) 'Privacy "Myths" Listed by the U.S. Government Aren't So Mythical', American Civil Liberties Union and Friends of Privacy. Available online at https://www.aclu.org/files/assets/us_privacy_-_myths_and_realities.pdf, Accessed 15/06/2014.

Angwin, J. (2011) 'How Much Should People Worry About the Loss of Online Privacy? (15/11/2011)', *The Wall Street Journal*, Available online at http://www.wsj.com/articles/SB10001424052970204190704577024262567105738, Accessed 12/10/2012.

ANSII (2012) 'Core Missions', *http://www.ssi.gouv.fr/fr/anssi/missions/*, date accessed 19/07/2012.

Archick, K. (2016) 'US – EU Cooperation Against Terrorism (2/03/2016)', *Congressional Research Service*, Library of Congress. Available online at http://www.statewatch.org/news/2016/mar/usa-crs-eu-usa-c-tcooperation.pdf, Accessed 11/07/2016.

Baker, J. (2015) '"Progress made" as EU aims to get new data protection laws ASAP (15/07/2015)', *The Register*. Available online at http://www.theregister.co.uk/2015/07/15/negotiators_go_for_early_wins_in_new_eu_data_protection_law/, Accessed 11/09/2015.

Bamford, J. (2013) 'NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar (6/12/2013)', *Wired*. Available online at https://www.wired.com/2013/06/general-keith-alexander-cyberwar/, Accessed 11/02/2014.

Barlow, J. P. (1996) 'A Declaration of the Independence of Cyberspace', 9 February. Available at: https://projects.eff.org/~barlow/Declaration-Final.html, Accessed 18/09/2013.

Bateman, T. (2013) 'Police warning after drug traffickers' cyber-attack (16/10/2013)', *BBC News*, Available online at http://www.bbc.com/news/world-europe-24539417, Accessed 09/10/2015.

BBC News (2004) 'US cyber security chief resigns', *BBC News*. Available online at http://news.bbc.co.uk/2/hi/technology/3714412.stm, Accessed 23/06/2015.

BBC News (2015) 'Japan to allow military role overseas in historic move (18/09/2015)', *BBC News*, Available online at http://www.bbc.com/news/world-asia-34287362, Accessed 03/10/2015.

Behr et. al. (2013) 'Radicalisation in the digital era: the use of the internet in 15 cases of terrorism and extremism', Santa Monica, CA: RAND Corporation'. Available online at http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf, Accessed 17/04/2015.

Bendrath, R. (2004) 'The American Cyber Angst and the Real World – Any Link?' Paper presented at the annual meeting of the International Studies Association, 17 March, Le Centre Sheraton Hotel, Montreal, Quebec, Canada, available at: www.allacademic.com/meta/p73883_index.html, Accessed 12/12/2013.

Bertsch, J., Kaba, M., Quaintance, W., Rehtanz, C. (2001) 'Enhanced reliability and other benefits with online security assessment', Paper presented at the *Developments in Power System Protection, Seventh International Conference (IEE)*, (9-12 April).

Beshar, P. (2015) 'Cybersecurity's privacy problem (3/08/2015)', *Fortune*, Available online at http://fortune.com/2015/08/03/cybersecurity-privacy-europe-u-s/, Accessed 12/01/2016.

Bisson, D. M. (2014) 'Cyber Power Restrained: How Strategic Culture Inhibits the Integration of Cyber Weapons by the United States Military', *Senior Projects Spring 2014*. Paper 402. Available online at http://digitalcommons.bard.edu/senproj_s2014/402, Accessed 11/12/2014.

Bisson, D. M. (2015) ‘A “Cyber” Study of the U.S. National Security Strategy Reports (17/02/2015)’, *Tripwire*, Available online at http://www.tripwire.com/state-of-security/government/a-cyber-study-of-the-u-s-national-security-strategy-reports/, Accessed 03/04/2015.

Boehm, F., Andrees, M., Beaucamp, J., Hey, T. (2015) ‘A comparison between US and EU data protection legislation for law enforcement purposes’, Study, Policy Department C - Citizens' Rights and Constitutional Affairs, EU Parliament. Available online at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf, Accessed 23/02/2016.

Bölinger, M. (2014) ‘EU verdict rekindles Internet censorship debate (28/04/2014)’, Available online at http://www.dw.de/eu-verdict-rekindles-internet-censorship-debate/a-17526954, Accessed 11/06/2014.

Boué, T. (2015) ‘Closing the gaps in EU cybersecurity: Let’s get it right (05/03/2015)’, *EurActiv*, Available online at http://www.euractiv.com/sections/infosociety/closing-gaps-eu-cybersecurity-lets-get-it-right-312652, Accessed 16/04/2015.

Bowman, C. M. (2016) ‘German DPA Plans to Challenge Privacy Shield (16/08/2016)’, *The National Law Review*. Available online at http://www.natlawreview.com/article/german-dpa-plans-to-challenge-privacy-shield, Accessed 18/08/2016.

Brewster, T. (2014) ‘Europol launches taskforce to fight world’s top cybercriminals (1/09/2014)’, *The Guardian*, Available online at https://www.theguardian.com/technology/2014/sep/01/europol-taskforce-cybercrime-hacking-malware, Accessed 11/02/2015.

BSI (2014) ‘Die Lage der IT-Sicherheit in Deutschland 2014’, *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, Available online at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile, Accessed 11/08/2015.

Bucci, S. P., Rosenzweig, P., & Inserra, D. (2013) ‘A Congressional Guide: Seven Steps to US Security, Prosperity, and Freedom in Cyberspace (28/03/2013)’, *The Heritage Foundation,* Backgrounder, No. 2785. Available online at http://s3.amazonaws.com/thf_media/2013/pdf/bg2785.pdf, Accessed 9/07/2014.

Bunyan, T. (2013) ‘How the EU works and justice and home affairs decision-making’, *Statewatch*. Available online at http://www.statewatch.org/analyses/no-205a-cleu.pdf, Accessed 12/08/2014.

Burke, E. (2001) The expanding importance of the computer fraud and abuse act. *GigaLaw.*

Bush, G. W. (2001a) ‘Remarks by the President Upon Arrival’, Office of the Press Secretary, The White House. Available online at https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010916-2.html, Accessed 11/10/2012.

Bush, G. W. (2001b) ‘Executive Order 13228 - Establishing the Office of Homeland Security and the Homeland Security Council (8/10/2001)’, Available online by

Gerhard Peters and John T. Woolley at *The American Presidency Project*. http://www.presidency.ucsb.edu/ws/?pid=61509. Accessed 16/03/2014.

Bush, G. W. (2001c) Executive Order No. 13231 – Critical Infrastructure Protection in the Information Age (16/10/2001)', Available online at https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf, Accessed 16/03/2014.

Bush, G. W. (2002) 'The national security strategy of the United States of America', Executive Office of the President. Washington DC: The White House.

Bush, G. W. (2003) 'The National Strategy to Secure Cyberspace', The White House, Washington, D.C.: U.S. Government Printing Office.

Business Insurance (2013) 'European Parliament approves cyber security mandate' by Judy Greenwald, available at: www.businessinsurance.com/article/20130416/NEWS07/130419863, Accessed 5/06/2013.

Buxton, J., & Bingham, T. (2015) 'The rise and challenge of dark net drug markets', *Policy Brief*, *7*. Available online at http://www.drugsandalcohol.ie/23274/1/Darknet%20Markets.pdf, Accessed 17/02/2016.

Cabinet Office (2014) 'Cyber skills for a vibrant and secure UK (12/12/2014)', Available online at https://www.gov.uk/government/news/cyber-skills-for-a-vibrant-and-secure-uk, Accessed 17/09/2015.

Cabinet Office (2016) 'The UK Cyber Security Strategy 2011-2016 (April 2016)', Available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf, Accessed 23/05/2016.

Caldwell & McLaughin (2014) 'Obama: U.S. to 'start going on some offense' in ISIS fight (9/10/2014)', *CNN Politics*, Available online at http://edition.cnn.com/2014/09/07/politics/obama-isis-speech/, Accessed 07/02/2015.

Caldwell, L. R. (2014) 'Assistant Attorney General Leslie R. Caldwell Speaks at Cybercrime 2020 Symposium', 4th December 2014, Washington, D.C. Available online at https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-cybercrime-2020-symposium, Accessed 12/04/2015.

Caldwell, L. R. (2015) 'Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the Georgetown Cybersecurity Law Institute', 20th May 2015, Washington, D.C. Available online at https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-georgetown-cybersecurity, Accessed 12/08/2015.

Cardoso Reis, B. (2009) 'Europeans are from Athens: European Strategic Culture and the deepening of ESDP in an enlarged EU', in *Paper based on discussions held at the Lisbon conference on "New Perspectives for European Security", EU-Consent*. Available online at http://www.eu-consent.net/library/deliverables/D161.pdf, Accessed 14/10/2014.

Carson, K. (2011) 'Taylorism, Progressivism, and Rule by Experts (24/08/2011)', Foundation for Economic Foundation. Available online https://fee.org/articles/taylorism-progressivism-and-rule-by-experts/, Accessed 17/11/2013.

Carson, K. A. (2010) 'The Thermidor of the Progressives: Managerialist Liberalism's Hostility to Decentralised Organisation', *Centre for a Stateless Society, Paper*, *9*. Available online at https://www.academia.edu/1605410/The_Thermidor_of_the_Progressives?auto=download, Accessed 23/10/2014.

Castelli, J. Christopher, (2014) 'Review aimed at framework for cyber stability plows familiar ground (7/06/2014)', *Inside Cyber Security*, Available online at http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content/review-aimed-at-framework-for-cyber-stability-plows-familiar-ground/menu-id-1089.html, Accessed 24/08/2014.

Cavelty, M. D. (2012) 'The militarisation of cyberspace: Why less may be better', In *2012 4th International Conference on Cyber Conflict (CYCON 2012)* IEEE. Available online at https://ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf, Accessed 7/01/2013.

Chabinsky, S. (2010) 'Speech by Steven R. Chabinsky', Available online at https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom, Accessed 12/02/2013.

Chatham House (2014) Cyber security: Building Resilience, Reducing Risks, 19-20 May 2014, Chatham House, London.

Chaudry, A. (2012) 'A politicized civil service? (23/11/2012)', *Dawn*, Available online at http://www.dawn.com/news/766177/a-politicised-civil-service, Accessed 27/08/2015.

Cirlig, C.C. (2014) 'Cyber defence in the EU Preparing for cyber warfare?', *European Parliamentary Research Service*, European Parliament Briefing. Available online at http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf, Accessed 11/02/2015.

Clinton, W. J. (1998) *A National Security Strategy for a New Century.* Washington, DC: US Government Printing Office.

Commission of the European Communities (1993) 'Growth, Competitiveness, Employment. The challenges and Ways forward into the 21st century. White Paper' COM (93) 700, 5 December, available at: http://europa.eu/documentation/officialdocs/whitepapers/pdf/growth_wp_com_93_700_parts_a_b.pdf. Accessed 12/02/2013.

Connolly, K. (2012) 'Twitter blocks neo-Nazi account in Germany (18/10/2012)', *The Guardian*, Available online at http://www.theguardian.com/technology/2012/oct/18/twitter-block-neo-nazi-account, Accessed 14/02/2013.

Connolly, K. (2015) 'German secret service BND reduces cooperation with NSA (07/05/2015)', *The Guardian*, Available online at http://www.theguardian.com/world/2015/may/07/german-secret-service-

bnd-restricts-cooperation-nsa-us-online-surveillance-spy, Accessed 09/10/2015.

Cook, J. and Price, R. (2015) 'Europe's highest court just rejected the 'safe harbor' agreement used by American tech companies (06/10/2015)', *Business Insider*, Available online at http://uk.businessinsider.com/european-court-of-justice-safe-harbor-ruling-2015-10, Accessed 14/11/2015.

Council of Europe (2010) 'Convention for the Protection of Human Rights', as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13, European Court of Human Rights. Available online at http://www.echr.coe.int/Documents/Convention_ENG.pdf, Accessed 19/02/2014.

Council of Europe (2016) Budapest Convention on Cybercrime, Treaty No.185, Available online at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, Accessed 04/05/2016.

Council of the EU (1999) 'Council Decision of 3 December 1998 instructing Europol to deal with crimes committed or likely to be committed in the course of terrorist activities against life, limb, personal freedom or property', (1999/C 26/06). Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.1999.026.01.0022.01.ENG&toc=OJ:C:1999:026:TOC. Accessed 23/11/2014.

Council of the EU (2009) 'EU-US Statement on "Enhancing transatlantic cooperation in the area of Justice, Freedom and Security",' at the EU-US JHA Ministerial meeting in Riga. Available online at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015184%202009%20INIT, Accessed 23/01/2014.

Council of the EU (2014) 'Council conclusions on Afghanistan (23/06/2014)', Available online at http://eeas.europa.eu/delegations/afghanistan/documents/content/eu-strategy-2014-2016_en.pdf, Accessed 9/02/2015.

Council of the EU (2015) 'First EU-wide rules to improve cybersecurity: deal with EP (08/12/2015)', EU Council, 904/15. Available online at http://www.consilium.europa.eu/en/press/press-releases/2015/12/08-improve-cybersecurity/, Accessed 08/01/2016.

Cross, M.K.D. (2011) 'EU Intelligence Sharing & The Joint Situation Centre: A Glass Half-Full', Meeting of the European Union Studies Association March 3-5, 2011. Available online at http://www.offiziere.ch/wp-content/uploads/3a_cross.pdf, Accessed 12/04/2013.

Curtis, S. (2014) 'Eugene Kaspersky: traditional crime 'is coming to cyberspace' (30/09/2014)', *The Telegraph*, Available online at http://www.telegraph.co.uk/technology/internet-security/11118866/Eugene-Kaspersky-traditional-crime-is-coming-to-cyberspace.html, Accessed 15/09/2015.

Cyber Intelligence Europe (2014) Conference, Intelligence–Sec. 22-24 September 2014, Brussels.

Department for Business Innovation and Skills (2013) 'Call for evidence on a preferred standard in cyber security – Government response', Department for Business Innovation and Skills, Available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262114/bis-13-1308-call-for-evidence-on-preferred-standard-in-cyber-security-response.pdf, Accessed 15/02/2015.

Department of Defence (2011) 'Strategy for Operating in Cyberspace', July 2011, Department of Defence Strategy. Available online at http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf, Accessed 11/09/2012.

Department of Defence (2015) 'The DOD Cyber strategy', Department of Defence. Available online at http://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, Accessed 13/12/2015.

Department of Defence (DBS) (2004) Report of the Defence Science Board Task Force on Strategic Communication, Available online at http://fas.org/irp/agency/dod/dsb/commun.pdf, Accessed 03/04/2015.

Department of Defence (DoD) (1979) 'DoD 5200. 28-M ADP Security Manual Techniques and Procedures or Implementing, Deactivating, Testing and Evaluating', http://biotech.law.lsu.edu/blaw/dodd/corres/pdf2/p520028m.pdf, Accessed 19/02/2013.

Department of Homeland Security (2014) 'Critical Infrastructure Cyber Community C³ Voluntary Program', Available online at https://www.dhs.gov/ccubedvp, Accessed 23/08/2015.

Department of Justice (2003) 'FY 2003 – 2008 Strategic Plan', U.S. Department of Justice. Available online at https://www.justice.gov/archive/mps/strategic2003-2008/message.pdf, Accessed 11/05/2015.

Department of Justice (2004) U.S. Southern District Court of New York (2004) 'Criminal Complaint against Kyle Fedorek (15/05/2014), Case 1:14-mj-01064-UA. Available online at https://www.cis.uab.edu/forensics/blog/kbello.kyle.fedorek.complaint.pdf, Accessed 7/10/2015.

Department of Justice (2014a) 'Accomplishments under the leadership of Attorney General Holder', Available online at https://www.justice.gov/accomplishments, Accessed 7/05/2015.

Department of Justice (2014b) 'FY 2014 Budget Request, Cyber Security', Available online at https://www.justice.gov/sites/default/files/jmd/legacy/2013/12/02/cyber-security.pdf, Accessed 3/04/2015.

Department of Justice (2014c) 'Manhattan U.S. Attorney And FBI Assistant Director-In-Charge Announce Charges In Connection With Blackshades Malicious Software That Enabled Users Around The World To Secretly And Remotely Control Victims' Computers (19/05/2014)', Press Release. Available online at https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection, Accessed 07/01/2015.

Department of Justice (2014d) 'The FBI Story 2014', FBI Office of Public Affairs.

Department of Justice (2015a) '9-50.000 - CHIP Guidance - 9-50.103 - Computer Crime & Intellectual Property Section'. Available online at https://www.justice.gov/usam/usam-9-50000-chip-guidance#9-50.103, Accessed 23/07/2015.

Department of Justice (2015b) 'FY 2015 Budget Request - Mutual Legal Assistance Treaty Process Reform', Available online at https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf, Accessed 13/11/2015.

Department of Justice and Equality (2015c) 'European Justice Ministers reach agreement on EU Passenger Name Record proposals (04/12/2015), Available online at http://www.justice.ie/en/JELR/Pages/PR15000627, Accessed 06/12/2015.

Department of Justice, *U.S. Attorney's Manual 9-50.103* Computer Crime & Intellectual Property Section, Available online at https://www.justice.gov/usam/usam-9-50000-chip-guidance#9-50.103, Accessed 07/06/2015.

Deutsche Welle (2013) 'Snowden ally Appelbaum claims his Berlin apartment was invaded (21/12/2013)', Deutsche Welle, Available online at http://www.dw.com/en/snowden-ally-appelbaum-claims-his-berlin-apartment-was-invaded/a-17315069, Accessed 13/02/2014.

Deutscher Bundestag (2012) Basic Law for the Federal Republic of Germany, Available online at https://www.bundestag.de/blob/284870/ce0d03414872b427e57fccb703634dcd/basic_law-data.pdf, Accessed 19/09/2015.

DG Justice (2016a) 'Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision (13/04/2016)', Article 29 Data Protection Working Party. Available online at http://ec.europa.eu/justice/data-protection/article29/documentation/opinionrecommendation/files/2016/wp238_en.pdf, Accessed 17/06/2016.

DG Justice (2016b) 'Reform of EU data protection rules', DG Justice. Available online at http://ec.europa.eu/justice/data-protection/reform/index_en.htm, Accessed 18/08/2016.

DG Justice (2016c) 'Signing of the "Umbrella" Agreement: A major step forward in EU-U.S. relations', DG Justice. Available online at http://ec.europa.eu/justice/newsroom/data-protection/news/160602_en.htm, Accessed 12/08/2016.

DG Justice and Consumers (2016d) 'The EU-U.S. Privacy Shield', EU Justice. Available online at http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm, Accessed 16/08/2016.

Dimov, D. (2013) 'Differences between the privacy laws in the EU and the US', Infosec Institute. Available online at http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/ Accessed 12/09/2014.

Dinkwater, D. (2014) 'EU's new cybercrime taskforce set to launch (21/07/2014)', *SC Magazine UK*, Available online at http://www.scmagazineuk.com/eus-new-cybercrime-taskforce-set-to-launch/article/361822/, Accessed 12/10/2015.

Doyle, Charles (2014) 'Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws (15/10/2014)', *Congressional Research Service*, Library of Congress. Available online at https://www.fas.org/sgp/crs/misc/97-1025.pdf, Accessed 11/05/2015.

Drummond and McClendon (2001) 'Cybercrime – alternative models for dealing with unauthorised use and abuse of computer networks', *Law and Internet* 3.

Dvorsak, A. (2012) 'Development of cyber defense strategies on the foundations of strategic culture-small countries perspective', Policy Paper, ETH Zürich.

EEAS (2014) 'EU-US cooperation on cyber security and cyberspace (16/03/2014)', Fact Sheet, 140326/01, Available online at https://eeas.europa.eu/statements/docs/2014/140326_01_en.pdf, Accessed 12/08/2014.

Electronic Privacy Information Center, 'National Information Infrastructure Protection Act of 1996', H.R.3723, Available online at https://epic.org/security/1996_computer_law.html, Accessed 16/07/2015.

Elkins, D. J., & Richard E. B. Simeon (1979) 'A Cause in Search of Its Effect, or What Does Political Culture Explain?', *Comparative Politics*, *11*/2:127–145. Available online at http://doi.org/10.2307/421752, Accessed 03/04/2013.

ENISA (2011) 'Cyber Atlantic – 3 November 2011', Available at: www.enisa.europa.eu/activities/ResilienceandCIIP/cybercrisiscooperation/cyber-atlantic/cyber-atlantic-2011, Accessed 9/10/2012.

ENISA (2014) 'An evaluation Framework for National Cyber Security Strategies', by Dimitra Liveri and Anna Sarri, Available online at https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-securitystrategies/at_download/fullReport, Accessed 16/12/2014.

ENISA (2015) 'Critical Information Infrastructures Protection approaches in EU', *ENISA*. Available online at https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf, Accessed 19/11/2015.

ENISA (2016a) 'CIIP Governance in the European Union Member States (Annex)', ENISA. Available online at https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/ciip-governance-in-the-eu-annex, Accessed 23/05/2016.

ENISA (2016b) 'National Cyber Security Strategies (NCSSs) Map', *ENISA*, Available online at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map, Accessed 13/05/2016.

EU Commission (1999) 'eEurope - An information society for all', COM(1999) 687 final, Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24221, Accessed 15/04/2014.

EU Commission (2012) 'Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security (11/08/2012)', Official Journal

L 0215. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1416915581157&uri=CELEX:22012A0811(01), Accessed 09/01/2013.

EU Commission (2013) 'EU-US agreements: Commission reports on TFTP and PNR (27/11/2013)', Press Release. Available online at http://europa.eu/rapid/press-release_IP-13-1160_en.htm, Accessed 11/12/2013.

EU Commission (2014) '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', COM/2013/048 final - 2013/0027 (COD). Available online at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52013PC0048, Accessed 13/04/2014.

EU Commission (2016) 'Digital Single Market', Digital Economy and Society, Available online at https://ec.europa.eu/digital-single-market/en/digital-single-market, Accessed 1/07/2016.

EU Council (2002) 'Setting up Eurojust with a view to reinforcing the fight against serious crime', Council Decision 2002/187/JHA, Available online at http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejdecision/Eurojust%20Decision%20%28Council%20Decision%202002-187-JHA%29/Eurojust-Council-Decision-2002-187-JHA-EN.pdf, Accessed 14/02/2016.

EU Council (2008) 'Directive on European critical infrastructures: on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection', *Council Directive 2008/114/EC*, Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF, Accessed 03/01/2013.

EU Council (2015a) 'Common challenges in combating cybercrime (30/11/2015)', Eurojust/Europol Joint Paper, 14812/15, Available online at http://statewatch.org/news/2016/mar/eu-europol-eurojust-report-cybercrime-data-retention-14812-15.pdf, Accessed 13/02/2016.

EU Council (2015b) 'Data Protection: Council agrees on a general approach (15/06/2015)', Press Release, 450/15, Available at http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection/, Accessed on 05/08/2015.

EU Council (2016) 'EU-wide cybersecurity rules adopted by the Council (1705/2016)', *EU Council 251/16*, Available online at http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/, Accessed 26/05/2016.

EU Court of Justice (2015) 'The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid (06/10/2015)', No 117/15, Available online at http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf, Accessed 18/11/2015.

EU Parliament (2011) 'Cyber war and cyber security: challenges faced by the EU and its Member States', Directorate-General for External Policies. Available online athttp://www.evi.ee/lib/cyber.pdf?&lang=en_us&output=json&sessionid=851b4c640621b1f19d8fbb00504856e5, Accessed 05/05/2013.

EU Parliament (2013) 'Data and Security Breaches and Cyber-Security Strategies in the EU and its international counterparts', Directorate-General for Internal Policies, Policy Department A Economic and Scientific Policy, available at: www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE_NT%282013%29507476_EN.pdf, Accessed 12/10/2013.

EU Parliament (2014a) 'EU Internal Security Strategy and enhancing police cooperation', 19 March, Civil Liberties, Justice and Home Affairs (LIBE) Committee.

EU Parliament (2014b) European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading). Available online at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT%20TA%20P7-TA-20140212%200%20DOC%20XML%20V0//EN, Accessed 20/12/2014.

EU Parliament (2016) 'Internal Security Fund (2016 April)', How the EU budget is spent, *European Parliamentary Research Service*, European Parliament Briefing, Available online at http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/580897/EPRS_BRI(2016)580897_EN.pdf, Accessed 24/05/2016.

EU Parliament and Council (2013) 'Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA', *Official Journal L 218*, 2013, Available online at http://eur-lex.europa.eu/eli/dir/2013/40/oj, Accessed 12/09/2013.

EurActiv (2015a) 'Cyber security directive held up in face of 'Wild West' Internet (01/04/2015)', *EurActiv*, Available online at http://www.euractiv.com/sections/infosociety/cyber-security-directive-held-face-wild-west-internet-313431, Accessed 17/06/2015.

EurActiv (2015b) 'EU lawmakers, countries agree on cyber security law (08/12/2015)', *EurActiv*, Available online at http://www.euractiv.com/sections/digital/eu-lawmakers-countries-agree-cybersecurity-law-320212, Accessed 14/01/2016.

EurActiv (2015c) 'New EU cybersecurity rules to hit US internet firms (07/8/2015)', *EurActiv*, Available online at http://www.euractiv.com/sections/infosociety/new-eu-cybersecurity-rules-hit-us-internet-firms-316818, Accessed 13/08/2015.

Eurojust (2014) 'International operation hits BlackShades users (19/05/2014)', Available online at http://www.eurojust.europa.eu/press/pressreleases/pages/2014/2014-05-19.aspx, Accessed 12/03/2015.

Eurojust (2015a) 'Mission and tasks', *Eurojust*, Available online at http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx, Accessed 13/01/2016.

Eurojust (2015b) ‘Operation BlackShades: An evaluation’, April 2015. Available online at http://eurojust.europa.eu/press/Documents/2015-10-12_Blackshades-Case-Evaluation.pdf, Accessed 12/06/2015.

EUROPA (2010) Division of competences within the European Union, Summaries of EU legislation. Available online at http://europa.eu/legislation_summaries/institutional_affairs/treaties/lisbon_treaty/ai0020_en.htm#, date accessed 04/03/2012.

Europe and the Global Information Society (1994) ‘Bangemann report recommendations to the European Council’, 26 May, available at: www.epractice.eu/files/media/media_694.pdf, Accessed 12/02/2013.

European Commission (2001) ‘Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime’, Communication to the European Parliament and Council, COM (2000) 890 final, 26 January 2001.

European Commission (2006) ‘European Programme for Critical Infrastructure Protection’, 12 December, Available at: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm, Accessed 09/10/2012.

European Commission (2007) ‘Towards a general policy on the fight against cyber crime’, 22 May, Available online at: http://ec.europa.eu/homeaffairs/policies/crime/crime_cybercrime_en.html, Accessed 24/11/2012.

European Commission (2009) ‘Protecting Europe from Large Scale Cyber attacks and Cyber disruptions: Enhancing Preparedness, Security and Resilience’, 30 March, available at: http://europa.eu/legislation_summaries/information_society/internet/si0010_en.htm, Accessed 9/06/2012.

European Commission (2010a) ‘EU–US Summit 20 November 2010 – Joint Statement’, MEMO/10/597. Available at: http://europa.eu/rapid/press-release_MEMO-10-597_en.htm, Accessed 14 September 2012.

European Commission (2010b) ’A Digital Agenda for Europe’, Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2010) 245.

European Commission (2010c) ‘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’, COM (2010) 673 Final, Brussels, 22 November (Brussels: European Commission).

European Commission (2010d) ‘EUROPE 2020 – A Strategy for Smart, Sustainable and Inclusive Growth’, COM (2010) 2020.

European Commission (2013a) ‘Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’, COM (2013) 1 final, Brussels, 7 February.

European Commission (2013b) ‘EU–US cooperation on Cyber security and Cybercrime’, 30 April, SPEECH/13/380, available at:

http://europa.eu/rapid/press-release_SPEECH-13-380_en.htm, Accessed 6 May 2013.

European Commission (2013c) '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', 2013/0027(COD), Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF, Accessed 21 July 2013.

European Commission (2013d) Joint Review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security SEC(2013)630final, Brussels 27/11/2013, Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0844:FIN:EN:PDF, date accessed 29/11/2013.

European Commission (2014a) 'Progress on EU data protection reform now irreversible following European Parliament vote (12/03/2014)', MEMO/14/186, Available online at http://europa.eu/rapid/press-release_MEMO-14-186_en.htm, Accessed 15/03/2014.

European Commission (2014b) 'Speech: A data protection compact for Europe (28/01/2014)', Speech/14/62, Available online at http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm, Accessed 30/01/2014.

European Commission (2015) 'Agreement on Commission's EU data protection reform will boost Digital Single Market', IP/15/6321. Available online at http://europa.eu/rapid/press-release_IP-15-6321_en.htm, Accessed 12/01/2016.

European Commission (2016a) 'EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield (02/02/2016)', IP/16/216, Available online at http://europa.eu/rapid/press-release_IP-16-216_en.htm, Accessed 19/03/2016.

European Commission (2016b) 'Fact Sheet, EU-U.S. Privacy Shield (29/02/2016)', MEMO/16/434, Available online at http://europa.eu/rapid/press-release_MEMO-16-434_en.htm, Accessed 19/03/2016.

European Council (2013) 'Report of the EU-U.S. Working Group on data protection (16/11/2013)' Doc. 16987/13.

European Parliament (2013a) 'Report on the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (22/11/2013)', Document n.A7-0403/2013. http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0403&language=EN, date accessed 25/11/2013.

European Parliament (2013b) 'Working Document 4 on US Surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation (10/12/2013)', Available online at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd4_1011371/WD4_1011371EN.pdf, date accessed 13/12/2013.

European Parliament (2014) 'Subject: VP/HR — EU offensive capabilities', Answer given by High Representative/Vice-President Ashton on behalf of the Commission. Available online at E-013235-13, http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-013235&language=EN, Accessed 20/03/2014.

European Parliamentary Research Service (EPRS) (2013) 'EU approach to cyber-security', by Francesca Ferraro, Members' Research Service, 31 March, Available online at: www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140775/LDM_BRI(2014)140775_REV1_EN.pdf, last accessed 2/04/2014.

European Security Strategy (2003) 'A Secure Europe in a Better World (07/12/2003)', Brussels, Available online at http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf, date accessed 13/10/2012.

Europol (2013) 'Hackers deployed to facilitate drugs smuggling (June 2013)', *Cyber Bits*, Available online at https://www.europol.europa.eu/sites/default/files/publications/cyberbits_04_ocean13.pdf, Accessed 07/10/2015.

Europol (2014a) 'Expert international cybercrime taskforce is launched to tackle online crime', Available at: https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime, Accessed 12/10/2014.

Europol (2014b) 'The Internet Organised Crime Threat Assessment (iOCTA)', Available at: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta, Accessed 22/09/2015.

Europol (2015a) 'EC3 and Anubisnetworks Initiative Cooperation in Fighting Malware Threats Available at: https://www.europol.europa.eu/newsletter/ec3-and-anubisnetworks-initiate-cooperation-fighting-malware-threats, Accessed 20/12/2015.

Europol (2015b) 'The Internet Organised Crime Threat Assessment (iOCTA)', Available online at https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015, Accessed 14/12/2015.

Faber, P. (2012) 'Bringing Back Strategic Culture and Grand Strategy (16/04/2012)', International Relations and Security Network, ISN Podcast, ETH Zurich. Available online at http://www.multimedia.ethz.ch/episode_play/?doi=10.3930/ETHZ/AV-e17da76b-8acf-41cc-ac94-7ac3f047de3a, Accessed 17/01/2013.

Fafinski, S., Dutton, W. H., & Margetts, H. Z. (2010) Mapping and measuring cybercrime, *Oxford Institute Forum Discussion Paper*, No 18., Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1694107, Accessed 23/11/2012.

Farrell, H. (2015) 'What's new in the U.S. cyber strategy (24/04/2015)', *The Washington Post*. Available online at https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/04/24/whats-new-in-the-u-s-cyber-strategy/, Accessed 23/09/2015.

Farrell, H. (2016) 'Promoting Norms for Cyberspace (April 2015)', Cyber Brief, *Council on Foreign Relations*, Available online at http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358, Accessed 17/02/2016.

FBI (2003) Timeline of FBI History, https://www2.fbi.gov/libref/historic/history/historicdates.html, Accessed 3/07/2015.

FBI (2015) 'FBI Works with Foreign Partners to Target Botnet (9/04/2015)', *Press Release*. Available online at https://www.fbi.gov/news/pressrel/press-releases/fbi-works-with-foreign-partners-to-target-botnet, Accessed 11/10/2015.

Fidler, D. (2015) 'U.S. – China cyber deal takes norm against economic espionage global (28/09/2015)', Available online at http://blogs.cfr.org/cyber/2015/09/28/u-s-china-cyber-deal-takes-norm-against-economic-espionage-global/, Accessed 02/10/2015.

Finklea, K. M., & Theohary, C. A. (2015) 'Cybercrime: conceptual issues for congress and US law enforcement (15/1/2015)', *Congressional Research Service*, Library of Congress. Available online at https://www.fas.org/sgp/crs/misc/R42547.pdf, Accessed 24/03/2015.

Fischer, E. A. (2013 June) 'Federal laws relating to cybersecurity: Overview and discussion of proposed revisions (20/06/2013)', *Congressional Research Service*, Library of Congress. Available online at https://www.fas.org/sgp/crs/natsec/R42114.pdf, Accessed 21/05/2014.

Fischer, E. A., Liu, E. C., Rollins, J., & Theohary, C. A. (2014) 'The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress', *Congressional Research Service*, Library of Congress. Available online at https://www.fas.org/sgp/crs/misc/R42984.pdf, Accessed 14/03/2015.

Fischer, P., (2010) '*Will Privacy Law in the 21st Century Be American, European, Or International*', Münich: GRIN Verlag. Available online at http://www.grin.com/en/e-book/187981/will-privacy-law-in-the-21st-century-be-american-european-or-international, Accessed 11/08/2014.

Fleming, J. (2015) 'Cyber security directive held up in face of 'Wild West' Internet (01/04/2015)', *EurActiv*, Available online at http://www.euractiv.com/sections/infosociety/cyber-security-directive-held-face-wild-west-internet-313431, Accessed on 06/05/2015.

Forum Europe (2014) The 2nd Annual European Cyber Security Conference, Brussels, 25 March 2014.

Gago, A. (2014) 'Keynote Session: Commission's perspectives on cyber security', The 2nd Annual European Cyber Security Conference, Brussels, 25 March 2014.

Gallagher, S. (2015) 'What the government should've learned about backdoors from the Clipper Chip (14/12/2015)', ArsTechnica, Available online at http://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/, Accessed 08/01/2016.

GAO (2014) ‘Maritime critical infrastructure protection (June 2014)’, Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate, *United States Government Accountability Office*, Available online at http://www.gao.gov/assets/670/663828.pdf, Accessed 24/11/2014.

Gartner Security & Risk Management Summit (2015) 8-11 June 2015. Available online at http://events.gartner.com/#/en/navigator/sec21/agenda, Accessed 13/06/2015.

Geers, K. (2011) ‘Sun Tzu and Cyber War (09/02/2011)’, Cooperative Cyber Defence Centre of Excellence, Available online at *www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf,* Accessed 17/06/2012.

Gellman, B. and Poitras, L. (2013) ‘U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program (07/06/2013)’, *The Washington Post*, Available online at http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, Accessed 07/11/2014.

Georgetown University Law Center (2015) Third Annual Cybersecurity Law Institute, Georgetown University Law Center, 20-21 May 2015, Washington, D.C.

German Criminal Code, in the version promulgated on 13 November 1998, Federal Law Gazette I p. 3322, last amended by Article 1 of the Law of 24 September 2013, Federal Law Gazette I p. 3671 and with the text of Article 6(18) of the Law of 10 October 2013, Federal Law Gazette I p 3799. Available online at https://www.gesetze-im-internet.de/englisch_stgb/german_criminal_code.pdf, Accessed 11/12/2015.

German Federal Ministry of Interior (2015) ‘IT and cyber security’, *Federal Ministry of Interior*. Available online at http://www.bmi.bund.de/EN/Topics/IT-Internet-Policy/IT-Cybersecurity/it-cybersecurity_node.html, Accessed 23/10/2015.

Gibbs, S. (2015) ‘What is 'safe harbour' and why did the EUCJ just declare it invalid? (6/10/2015)’, *The Guardian*, Available online at http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection, Accessed 7/10/2015.

Gjelten, T. (2013) ‘First Strike: US cyber warriors seize the offensive’, *World Affairs Journal*, January/February 2013. Available online at http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive, Accessed 18/02/2013.

Goldsmith, J. (2015) ‘What Explains the U.S.-China Cyber “Agreement”?’, *Lawfare*, Available online at https://lawfareblog.com/what-explains-us-china-cyber-agreement, Accessed 9/10/2015.

Greenberg, A. (2014) ‘Hacker Lexicon: What Is End-to-End Encryption? (25/11/2014), *Wired*. Available online at https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/, Accessed 12/07/2015.

Greer, S. C. (2000) The margin of appreciation: interpretation and discretion under the European Convention on Human Rights (Vol. 17). Council of Europe. Available online at http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf, Accessed 16/02/2016.

Griffin, A. (2015) 'European court rules 'Safe Harbour' treaty that saw Facebook hand over user data to US is invalid, after challenge by student (06/10/2015)', *The Independent*, Available online at http://www.independent.co.uk/life-style/gadgets-and-tech/news/european-court-rules-safe-harbour-treaty-that-saw-facebook-hand-over-user-data-to-us-is-invalid-a6681291.html, Accessed 07/10/2015.

Hamilton, D. S. (Ed.). (2010) 'Shoulder to Shoulder: Forging a Strategic US-EU Partnership', Center for Transatlantic Relations, The Paul H. Nitze School of Advanced International Studies, The Johns Hopkins University. Available online at http://www.pssi.cz/download/docs/68_shoulder-to-shoulder-forging-a-strategic-u-s-eu-partnership.pdf, Accessed 17/12/2013.

Hannigan, R. (2014) 'The web is a terrorist's command-and-control network of choice (3/11/2014)', *Financial Times*, Available online at https://next.ft.com/content/c89b6c58-6342-11e4-8a63-00144feabdc0, Accessed 12/09/2016.

Harding, C. (2015) 'Can a digital single market give Europe the lead? (August 2015)', *ComputerWeekly*, Available online at http://www.computerweekly.com/opinion/Can-a-digital-single-market-give-Europe-the-lead, Accessed 23/03/2016.

Harres, C. (2014) 'Obama Says Cyberterrorism Is Country's Biggest Threat, U.S. Government Assembles "Cyber Warriors"' *International Business Times*. Available at www.ibtimes.com/obama-says-cyberterrorism-countrys-biggest-threat-us-government-assembles-cyber-warriors-1556337, Accessed 20/02/2014.

Hayes, B., Jeandesboz, J., Ragazzi, F., Simon, S., Mitsilegas, V. (2015) 'The law enforcement challenges of cybercrime: are we really playing catch-up?', Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs. Available online at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf, Accessed 29/11/2015.

Healey, J. & Jordan K. (2014) 'NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow', Atlantic Council, Brent Scowcroft Center on International Security, Available online at https://www.ciaonet.org/attachments/26619/uploads, Accessed 12/01/2015.

Hickie, S., Abbott, C., Zaffran, R. (2014) 'Trends in Remote Control Warfare', in *New Ways of War: Is Remote Control Warfare Effective?*, The Remote Control Digest, October 2014. Available online at http://oxfordresearchgroup.org.uk/sites/default/files/Remote%20Control%20Digest.pdf, Accessed 19/01/2015.

HM Government (2014) Sexual Violence against Children and Vulnerable People National Group Progress Report and Action Plan, Available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/2

30443/Sexual_Violence_against_Children_and_Vulnerable_People.pdf, Accessed 14/03/2015.

Hollis, Duncan B., (2012) 'Stewardship versus Sovereignty? International Law and the Apportionment of Cyberspace' (March 19, 2012) *Canada Centre for Global Security Studies*, Cyberdialogue 2012: What Is Stewardship in Cyberspace?, *Temple University Legal Studies Research Paper,* No. 2012: 25.

Hoofnagle, Chris (2010) 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments', European Commission, DG JUST, Available online at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf, Accessed 07/06/2013.

Hopkins, N., Borger, J., Harding, L. (2013) 'GCHQ: inside the top secret world of Britain's biggest spy agency (2/08/2013)', *The Guardian*. Available online at https://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden, Accessed 17/03/2014.

Houdart, Jean-Baptiste (2013) 'EU cybersecurity policy: A model for global governance', ISN Security Watch, 7 March. Available at: http://isnblog.ethz.ch/isn-security-watch/eu-cybersecurity-policy-a-model-for-global-governance, Accessed 23/03/2013.

Hujer, M. and Stark, H. (2014) 'Former NSA Director: 'Shame On Us' (24/03/2014)', Available online at http://www.spiegel.de/international/world/spiegel-interview-with-former-nsa-director-michael-hayden-a-960389-2.html, Accessed 28/12/2015.

Human Rights Watch (2015) 'France: Bill Opens Door to Surveillance Society (6/04/2015)', Available online at https://www.hrw.org/news/2015/04/06/france-bill-opens-door-surveillance-society, Accessed 26/06/2015.

ICSS 2015, The International Cyber Security Strategy Congress: "Cyber Security and Forensic Readiness, 4-5 February 2015, Leuven, Belgium.

InsideGov (2016) 'FY 2016 Agency Spending', *2016 United States Budget Estimate.* Available online at http://federal-budget.insidegov.com/l/119/2016-Estimate, Accessed 8/08/2016.

Internet Watch Foundation (2013) 'Internet watch foundation annual and charity report 2013', Available online at https://www.iwf.org.uk/assets/media/annual-reports/annual_report_2013.pdf.pdf, Accessed 12/10/2015.

Johnson, B. (2010) 'Privacy no longer a social norm, says Facebook founder (11/01/2010)', *The Guardian*, Available online at http://www.theguardian.com/technology/2010/jan/11/facebook-privacy, Accessed 11/08/2013.

Johnson, J. L., & Larsen, J. A. (2006) Comparative Strategic Culture Syllabus. Prepared for Defence Threat Reduction Agency Advanced Systems and Concepts Office, Available online at https://fas.org/irp/agency/dod/dtra/syllabus.pdf, Accessed 12/01/2014.

Jones, T. (2011) 'William Gibson: beyond cyberspace (22/09/2011)', *The Guardian*, Available online at https://www.theguardian.com/books/2011/sep/22/william-gibson-beyond-cyberspace, Accessed 23/05/2015.

Karas, T. H., Moore, J. H., & Parrott, L. K. (2008) 'Metaphors for cyber security', *Sandia Report SAND2008-5381. Sandia Labs, NM*.

Kaspersky, E. (2014) 'Ecosystem of cyber jungle', *ISCD Information and Cyber Security Conference*, 8-9 September 2014, Budapest

Kent, G. (2014) 'Sharing Investigation Specific Data with Law Enforcement-An International Approach (14/02/2014)', *Stanford Public Law Working Paper*. Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413, Accessed 14/12/2014.

Kerkhofs J., & Linthout P. Van (2013) 'The territorial competence (of collecting evidence) in cyberspace: A Belgian attempt to a solution (30/05/2013)', Available online at http://ec.europa.eu/enlargement/taiex/dyn/create_speech.jsp?speechID=30799&key=f518493f10dc48c00a75c5a83b53cc66, Accessed 9/01/2016.

King, R. (2014) 'Cyberattack on German Iron Plant Causes 'Widespread Damage': Report (18/12/2014)', *The Wall Street Journal*, Available online at http://blogs.wsj.com/cio/2014/12/18/cyberattack-on-german-iron-plant-causes-widespread-damage-report/, Accessed 11/08/2015.

Klare, M.T. (2015) 'Hard Power, Soft Power, and Energy Power: The New Foreign Policy Tool (3/3/2015)', *Foreign Affairs*. Available online at https://www.foreignaffairs.com/articles/united-states/2015-03-03/hard-power-soft-power-and-energy-power, Accessed 3/04/2015.

Klimburg (2015) 'Guest Post: Two years later, the EU's Cybersecurity Strategy stumbles forward (03/02/2015)', *Net Politics*, Council on Foreign Relations, Available online at http://blogs.cfr.org/cyber/2015/02/03/guest-post-two-years-later-the-eus-cybersecurity-strategy-stumbles-forward/, Accessed 17/06/2015.

Knake, R. (2015) 'Avoiding a game of He said, Xi said in cyberspace', Available online at http://blogs.cfr.org/cyber/2015/10/01/avoiding-a-game-of-he-said-xi-said-in-cyberspace/, Accessed 19/10/2015.

Krebs, B. (2015) 'Arrest of Chinese Hackers not a first for US', Krebs on Security, Available online at http://krebsonsecurity.com/2015/10/arrest-of-chinese-hackers-not-a-first-for-u-s/, Accessed 21/10/2015.

Krotonski, M. (2015) 'DOJ Cybercrime Efforts That Led To New Cybersecurity Unit', Law360. Available online at http://www.law360.com/articles/608408/doj-cybercrime-efforts-that-led-to-new-cybersecurity-unit, Accessed 03/01/2016.

Kujawa, A. (2012) 'You Dirty RAT! Part 2 – BlackShades NET (15/06/2012)', *Malwarebytes Lab*, Threat Analysis. Available online at https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-2-blackshades-net/, Accessed 19/11/2015.

Kuschewsky, M. (2015) 'EU – US Umbrella Agreement about to be concluded: towards a transatlantic approach to data protection? (10/09/2015)', *Inside Privacy*. Available online at https://www.insideprivacy.com/international/eu-us-umbrella-agreement-about-to-be-concluded-towards-a-transatlantic-approach-to-data-protection/, Accessed 19/10/2015.

Lagazio, Monica, Sherif, Nazneen and Cushman, Mike (2014) A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*: 58-74 Available online at http://eprints.lse.ac.uk/57000/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Cushman,%20M_Multi-level%20approach_Cushman_Multi-level%20approach_2014.pdf, Accessed 21/09/2014.

LEAP2015 (2015) Conference on cybercrime, 15 April 2015, Europol, Hague, The Netherlands.

Lee, P. (2014) 'How do EU and US privacy regimes compare? (05/03/2014)', *Privacy and information Law Blog*, Available online at http://privacylawblog.fieldfisher.com/2014/how-do-eu-and-us-privacy-regimes-compare, Accessed 7/08/2014.

Lewis, J. (2015) 'Cyber Security Breakfast Meeting, Discussion on the latest developments in cybersecurity as well as international cyber norms', ABA Standing Committee on Law & National Security, The University Club, 9 July 2015, Washington, D.C.

Limnéll, J. and Salonius-Pasternak C. (2012) 'Transatlantic Cyber Security', FIIA Briefing Paper 119, Available online at: http://www.fiia.fi/en/publication/303/transatlantic_cybersecurity/ Accessed 16/12/2012.

Lotrionte, C. (2015) 'Global Cybersecurity Perspectives', Third Annual Cybersecurity Law Institute, Georgetown University Law Center, 20-21 May 2015, Washington, D.C.

Lovett, E. J. (2015) 'Global Cybersecurity Perspectives', Third Annual Cybersecurity Law Institute, Georgetown University Law Center, 20-21 May 2015, Washington, D.C.

Lukasik, S. J. (1998) 'Review and Analysis of the Report of the President's Commission on Critical Infrastructure Protection', CISAC Working Paper, Stanford University, Available at: http://iis-db.stanford.edu/pubs/10300/lukasik1-98.pdf, Accessed 22/02/2014.

M. Haag (2015) 'The Northern District of California and the first CHIP Unit', U.S. Department of Justice, Available online at http://www.justice.gov/usao/priority-areas/cyber-crime/chip-units, Accessed 7/12/2015.

Mahnken, T. G. (2006) *United States Strategic Culture*. Prepared for the Defense Threat Reduction Agency Advanced Systems and Concepts Office. Science Applications International Corp. Washington D.C. Available online at http://www.au.af.mil/au/awc/awcgate/dtra/mahnken_strat_culture.pdf, Accessed 9/03/2015.

Mandiant (2013) 'APT1 Exposing One of China's Cyber Espionage Units (February 2013)', Available online at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, Accessed 26/07/2014.

Markus Funk, T. (2014) 'Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges', *Federal Judicial Centre*, International Litigation Guide, 1.

Martin, P. K. (2012) 'NASA Cybersecurity: An Examination of the Agency's Information Security', U.S. House of Representatives, Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology. Available online at https://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf, Accessed 25/10/2015.

Massé, E. (2015a) 'After the Paris attacks, France enacts sweeping legislation limiting fundamental freedoms (25/11/2015)', Available online at https://www.accessnow.org/after-the-paris-attacks-france-enacts-sweeping-legislation-limiting-fundamental-freedoms/, Accessed 28/11/2015.

Massé. E. (2015b) 'Feeding the All-Seeing Spider: France on verge of passing repressive new surveillance bill (27/04/2015)', Available online at https://www.accessnow.org/feeding-the-all-seeing-spider-france-on-verge-of-passing-repressive-new-sur/, Accessed 11/09/2015.

May, M., & Practical, G. S. E. C. (2004) 'Federal computer crime laws ', *The SANS Institute. Retrieved October*, *7*, 2005. Available online at https://www.sans.org/reading-room/whitepapers/legal/federal-computer-crime-laws-1446, Accessed 16/05/2015.

Miller, C. (2014) 'What we can learn from 1844's Post Office 'surveillance' scandal (21/03/2014)', *Wired*, Available online at http://www.wired.co.uk/news/archive/2014-03/21/post-office-espionage-scandal-1844, Accessed on 05/06/2014.

Nakashima, E. (2012) 'Obama signs secret directive to help thwart cyberattacks (14/11/2012)' in the *Washington Post*, Available online at: https://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html, Accessed 7/08/2013.

Nakashima, E. (2014) 'NSA phone record collection does little to prevent terrorist attacks, group says (12/01/2014)', The Washington Post. Available online at https://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-preventterroristattacksgroupsays/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html, Accessed17/02/2015.

Nakashima, E. and Goldman, A. (2015) 'CIA pulled officers from Beijing after breach of federal personnel records' *The Washingon Post*, Available online at https://www.washingtonpost.com/world/national-security/cia-pulled-officersfrombeijingafterbreachoffederalpersonnelrecords/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html, Accessed 13/10/2015.

NATO (2016) 'NATO and the European Union enhance cyber defence cooperation (10/02/2016)', NATO, Available online at http://www.nato.int/cps/en/natohq/news_127836.htm, Accessed 24/03/2016.

Nickolov, E. (2005) 'Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations' in *An International Journal*, 17: 105–19.

Noonan, W. (2014) 'Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future', Written testimony of USSS Cyber Operations Branch Criminal Investigative Division Deputy Special Agent in

Charge William Noonan for a Senate Committee on Appropriations, Subcommittee on Homeland Security hearing, U.S. DHS. Available online at https://www.dhs.gov/news/2014/05/07/written-testimony-usss-cyber-operations-branch-senate-appropriations-subcommittee, Accessed 11/08/2015.

Nye, J. S. (2010) 'Cyber Power', Belfer Center for Science and International Affairs, Harvard Kennedy School, available at: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf, Accessed 24/10/2011.

Obama, B. (2011) 'International Strategy for Cyberspace', White House, Available online at https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Accessed 08/09/2012.

OECD (2011) 'OECD Council Recommendation on Principles for Internet Policy Making (13/12/2011)', Available online at http://www.oecd.org/internet/ieconomy/49258588.pdf, Accessed 20/04/2015.

Oerting, T. (2014) 'Europol's mission to fight cyber crime (23/09/2014)', at *Cyber Intelligence Europe 2014 Conference*, Brussels.

OIG, Oxford Intelligence Group (2014) 'Workshop on 'Crime and the Internet', *OIG Seminar Series*, 2014 December.

Omand, D. (2015) 'Understanding digital intelligence and the Norms that might govern it', Centre for International Governance Innovation and Chatham House, Paper Series No. 8, March 2015 Available online at https://www.cigionline.org/sites/default/files/gcig_paper_no8.pdf, Accessed 19/06/2015.

Pearlman, A. R. (2010) 'Federal Cybersecurity Programs', New Federal Initiatives Project, 12 August 2010, Available online at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1655105*, date accessed 30/11/2012.

Pellerin, C. (2013) 'DOD Readies Elements Crucial to Cyber Operations (27/06/2013)', *DoD News*, American Forces Press Service, Department of Defence. Available online at http://archive.defense.gov/news/newsarticle.aspx?id=120381, Accessed 19/03/2015.

Peters, B. (1967) 'Security considerations in a multi-programmed computer system', In *Proceedings of the April 18-20, Spring Joint Computer Conference* (pp. 283-286). ACM.

Pew Research Center (2015) 'America's Changing Religious Landscape (12/05/2015)', Available online at http://www.pewforum.org/files/2015/05/RLS-05-08-full-report.pdf, Accessed 18/07/2015.

Polatin-Reuben, D., & Wright, J. (2014) 'An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet', In *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*. USENIX Association.

Police Executive Research Forum (2014) 'The role of local law enforcement agencies in preventing and investigating cyber crime', *Critical Issues in Policy Series*, Available online at http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf, Accessed 24/06/2015.

Pop, V. (2015) 'EU Interior Ministers Reach Deal on Air Passenger Data (04/12/2015), *The Wall Street Journal*, Available online at http://www.wsj.com/articles/eu-interior-ministers-try-to-come-to-deal-on-air-passenger-data-1449225830, Accessed 05/12/2015.

Porcedda, M. G. (2011) 'Transatlantic approaches to cybersecurity and cybercrime' in Chaillot Paper, No. 127, *The EU–US security and justice agenda in action*. Paris: EUISS.

Presidential Decision Directive (1998) 'Critical Infrastructure Protection - PDD-63', The White House, Washington, D.C. Available online at http://fas.org/irp/offdocs/pdd/pdd-63.htm, Accessed 24/11/2012.

Pulliam S. & Olsen T. (2008) 'Q & A: Barack Obama', *Christianity Today*, Available online at http://www.christianitytoday.com/ct/2008/januarywebonly/10432.0.html?start=2, Accessed 10/06/2015.

PwC (2016a) 'Cybercrime: Global Economic Crime Survey 2016', PwC, Available online at http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/cybercrime.html, Accessed 23/05/2016.

PwC (2016b) 'Global Economic Crime Survey 2016: The UK Old Dogs, New Tricks', *PwC*, Available online at http://www.pwc.co.uk/forensic-services/assets/gecs/gecs-uk-brochure-2016.pdf, Accessed 14/05/2016.

PwC & C.S.O. Magazine (2014) '2014 U.S. State of Cybercrime Survey', co-sponsored by the USSS, Software Engineering Institute CERT Program at Carnegie Mellon University and PwC. Available online at http://www.pwc.com/us/en/increasingiteffectiveness/publications/assets/pwc-2014-us-state-of-cybercrime.pdf, Accessed 29/02/2015.

Quinn, R. (2014) 'The FBI's Role in Cyber Security (16/06/2014)', Statement before the House Homeland Security Committee, Subcommittee on Cyber Security, Infrastructure Protection, and Security Technologies. Washington, D.C. Available online at https://www.fbi.gov/news/testimony/the-fbis-role-in-cyber-security, Accessed 08/03/2015.

Raicu, I., & Zeadally, S. (2003, February) 'Evaluating IPv4 to IPv6 transition mechanisms', In *Telecommunications, 2003. ICT 2003. 10th International Conference on* (2: 1091-1098). IEEE.

Raitman, R., Ngo, L., Augar, N. & Zhou, W. L. (2005) '*Security in the online e-learning environment*', Paper presented at the *5th IEEE International Conference on Advanced Learning Technologies*, Australia (5-8 July).

Reitano, T., Oerting, T., & Hunter, M. (2015) 'Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce',

The European Review of Organised Crime 2/2: 142-154. Available online at http://s3.amazonaws.com/academia.edu.documents/39045137/08_ReitanoEtAl_pp142154.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1469798523&Signature=KG8O%2Fe7%2BrImU3KeJSd5hDNho%2BgQ%3D&responsecontentdisposition=inline%3B%20filename%3DInnovations_in_International_Cooperation.pdf, Accessed 13/01/2016.

Roehrig W. (2014) 'How to integrate cyber threat intelligence into EU-led military operations', Cyber Intelligence Europe, Brussels, 23 September 2014.

Rogers, M. (Admiral) (2015) 'Cybersecurity for a New America: Big Ideas and New Voices', *New America*, Available online at http://www.newamerica.org/cybersecurity-initiative/events/cybersecurity-for-a-new-america/, Accessed 16/10/2015.

Rollins, J., & Henning, A. (2009) 'Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations', *Congressional Research Service*, Library of Congress. Available online at https://www.fas.org/sgp/crs/natsec/R40427.pdf, Accessed 35/06/2014.

Rossi, B. (2014) 'How to comply with the new EU Data Protection Regulation (13/10/2014)', *Information Age*, Available online at http://www.information-age.com/it-management/risk-and-compliance/123458546/how-comply-new-eu-data-protection-regulation, Accessed on 13/12/2014.

Samani, R. and Weafer, V. (2015) 'Takedown Stops Polymorphic Botnet (9/04/2015)', *McAfee Labs*. Available online at https://blogs.mcafee.com/mcafee-labs/takedown-stops-polymorphic-botnet/, Accessed 23/11/2015.

Sanger, D. & Mazzetti, M. (2013) 'Security Leader Says U.S. Would Retaliate Against Cyberattacks (12/03/2013)', *The New York Times*, Available online at http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?_r=0, Accessed 05/04/2013.

Santer, J. (1995) Speech by President Santer to the European Parliament, 17 January 1995, Speech/95/1, European Commission, Brussels. Available at http://www.cvce.eu/content/publication/1999/1/1/926b1836-f264-408c-915a-92671abc839a/publishable_en.pdf, Accessed 16/03/2015.

Segal, A. (2015) 'Attribution, Proxies and US-China Cyber Security Agreement', Net Politics, Council on Foreign Relations. Available online at http://blogs.cfr.org/cyber/2015/09/28/attribution-proxies-and-u-s-china-cybersecurity-agreement/, Accessed 13/10/2015.

Sensenbrenner, J. (2015) 'U.S. and Europe Forge Data-Protection Deal for Terrorism Cases (8/09/2015)', Available online at http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=397868, Accessed on 14/09/2015.

Serious Organised Crime Agency (SOCA) (2013) 'Cyber Crime', *SOCA,* Available online at http://www.soca.gov.uk/threats/cyber-crime, Accessed 28/01/2013.

Shadowserver Foundation (2015) 'AAEH/Beebone Botnet'. Available online at https://aaeh.shadowserver.org, Accessed 17/11/2015.

Sheftalovich, Z. (2016) 'The court case that could sink safe harbor (01/04/16)', *Politico*, Available online at http://www.politico.eu/article/the-court-case-that-could-sink-safe-harbor-microsoft-department-of-justice-data-protection-ireland/, Accessed 29/04/2016.

Shinder (2011) 'What makes cybercrime laws so difficult to enforce (26/01/2011)', Available online at http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/, Accessed 24/01/2013.

Siebel, H. (2014) 'Transcript: ARD interview with Edward Snowden', The Courage Foundation. Available online at https://edwardsnowden.com/2014/01/27/video-ard-interview-with-edward-snowden/, Accessed 19/01/2015.

Sieber, U. (1998) Legal aspects of computer-related crime in the information society. *University of Würzburg. COMCRIME - Study Prepared for the European Commission*. Available online at http://www.oas.org/juridico/english/COMCRIME%20Study.pdf, Accessed 2/06/2015.

Skaar, O. (2014) 'The World's 5 Most Prolific Cyber Armies (21/07/2014)', Available online at https://curiousmatic.com/worlds-5-prolific-cyber-armies/, Accessed 12/05/2015.

Smith, C. (2015) 'Hackers cash out directly from ATMs, don't need to steal your card first '25/09/2015)', Available online at http://bgr.com/2015/09/25/greendispenser-atm-malware-cash/, Accessed 2/10/2015.

Solana, J. (2003) 'A Secure Europe in a Better World: European Security Strategy (11/02/2003)', Civilian Perspective or Security Strategy, http://www2.weed-online.org/uploads/eu_civilian_perspective_2005.pdf#page=54, Accessed 10/10/2012.

Sophos Security Threat Report (July 2008) Available online at https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophossecurityreportjul08srna.pdf?la=en.pdf, Accessed 11/09/2014.

Spiegel 'NSA Experts: 'National Security Has Become a State Religion' (04/07/2014)', by Sven Becker, M. Rosenbach, J. Schindler, Available online at http://www.spiegel.de/international/world/interview-with-nsa-experts-on-us-spying-in-germany-a-979215.html, Accessed 03/02/2015.

Stanford News (2015) 'The day President Obama came to Stanford (13/02/2015)', Stanford News, Available online at http://news.stanford.edu/2015/02/13/summit-day-blog-021315/, Accessed 24/03/2015.

Statewatch (2015) 'Agreement between the US and the EU on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses (Umbrella Agreement)', Statewatch. Available online at http://statewatch.org/news/2015/sep/eu-us-umbrella-agreement-full-text.pdf. Accessed 17/01/2016.

Statista (2015) 'Number of full-time Google employees from 2007 to 2015', *Statista.* Available online at http://www.statista.com/statistics/273744/number-of-full-time-google-employees/, Accessed 9/11/2015.

Stone, E. (2006) 'Comparative strategic cultures literature review (part 1) (31/10/2006)', *Centre for Contemporary Conflict*. Comparative Strategic Cultures Curriculum Project. Available online at http://flp.fas.org/irp/agency/dod/dtra/stratcult-comp.pdf, Accessed 12/01/2014.

Stone, E. L., Twomey, C. P., & Lavoy, P. R. (2005) 'Comparative Strategic Culture, Strategic Insights', Conference Report, Monterey, California: Naval Postgraduate School. Available online at http://calhoun.nps.edu/handle/10945/29623, Accessed 12/01/2014.

Superville and Mendoza (2015) 'Obama calls on Silicon Valley to help thwart cyber attacks (13/02/2015)', *Phys.org*, Available online at http://phys.org/news/2015-02-obama-focus-cybersecurity-heart-silicon.html, Accessed 30/07/2016.

Symantec (2015) 'Internet Security Threat Report', *Symantec*, Available online at https://know.elq.symantec.com/LP=1542, Accessed 19/09/2015.

Tadjdeh, Y. (2013) 'Fears of Devastating Cyber-Attacks on Electric Grid, Critical Infrastructure Grow', *NDIA's Business and Technology Magazine*. Available online at http://www.nationaldefensemagazine.org/archive/2013/October/pages/FearsofDevastatingCyber-AttacksonElectricGrid,CriticalInfrastructureGrow.aspx, Accessed 7/03/2014.

Techau, J. (2016) 'EU Global Strategy: Defining Foreign Policy Interests (15/01/2016), *Carnegie Europe*, European Union Institute for Security Studies, Available online at http://carnegieeurope.eu/2016/01/15/eu-global-strategy-defining-foreign-policy-interests/it0r, Accessed 19/05/2016.

Terlikowski M. & Vyskoc, J. (2013) 'Coming to Terms with a New Threat: NATO and Cyber-Security (17/02/2013)', *Globsec Policy Institute*. Available online at http://www.cepolicy.org/publications/coming-terms-new-threat-nato-and-cyber-security, Accessed 11/09/2013.

The Guardian (2013) 'MI5 and industry join forces to fight cybercrime', The Guardian, Available online at https://www.theguardian.com/technology/2013/mar/27/mi5-industry-join-forces-cyber-crime, Accessed 11/02/2014.

Thompson, S. & R. Dossa, M. (2015) 'EU and U.S. reach "Umbrella Agreement" on data transfers (14/09/2015)', *Lexology*, Available online at http://www.lexology.com/library/detail.aspx?g=422bca41-2d54-4648-ae57-00d678515e1f, date accessed 17/09/2015.

Timmers, P. (2015) 'Cyber Security Strategies', ICSS 2015, The International Cyber Security Strategy Congress: "Cyber Security and Forensic Readiness, Leuven, 4 February 2015. Available online at https://www.b-ccentre.be/ICSS2015/sites/default/files/4feb%2011h30%20panel%201%20Paul%20Timmers.pdf, Accessed 11/02/2015.

Tucker, J. B. (2002) 'Putting Teeth in the Biological Weapons Convention (27/11/2013)', Can We Cope if the Lights Go Out? Issues in *Science and Technology*, Spring 2002, http://issues.org/18-3/tucker/, Accessed 27/05/2014.

Twitter (2015) 'Guidelines for law enforcement', Twitter. Available online at https://support.twitter.com/articles/41949, Accessed 13/02/2016.

U.S. Constitution (1791) 'Fourth Amendment', Bill of Rights. Available online at http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html, Accessed 21/06/2015.

U.S. Post Office Department (1921) Government Control and Operation of Telegraph, Telephone and Marine Cable Systems, August 1, 1918, to July 31, 1919: Acts of Congress, Proclamations of President, General Orders of Postmaster General, Reports on Administration of Wires, U.S. Government Printing Office, Original from the New York Public Library, Digitized on 09/10/ 2008.

U.S. State Department (2013) 'Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States (9/10/2012)', Available online at http://photos.state.gov/libraries/useu/231771/PDFs/Five%20Myths%20Regarding%20Privacy%20and%20Law%20Enforcement_October%209_2012_pdf.pdf, Accessed 17/02/2013.

U.S. Supreme Court, 'Hoke v. United States', 227 U.S. 308 (1913) https://supreme.justia.com/cases/federal/us/227/308/case.html,

UK Cabinet Office (2011) 'The UK Cyber Security Strategy: Protecting and promoting the UK in the digital world (November 2011)', *http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy/*, Accessed 13/06/2012.

UK Department for Business and Innovation (2013) 'Call for evidence on a preferred standard in cyber security: government response (Nov. 2013)', Dep. for Business and Innovation. Available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262114/bis-13-1308-call-for-evidence-on-preferred-standard-in-cyber-security-response.pdf, Accessed 30/10/2015.

UK Home Affairs (2013) 'Written evidence for E-crime Inquiry', Home Affairs Committee, Available online at http://www.parliament.uk/documents/commons-committees/home-affairs/120828%20eCrime%20evidence.pdf, Accessed 14/02/2013.

UN News Centre (2015) 'Billions of people in developing world still without Internet access, new UN report finds (21/09/2015)', Available online at http://www.un.org/apps/news/story.asp?NewsID=51924, Accessed 11/10/2015.

US Department of Commerce, NIST (2013) 'Preliminary Cybersecurity Framework – Improving Critical Infrastructure Cybersecurity Executive Order 13636', 22 October, Available online at http://nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf, Accessed 26/10/2013.

US Department of Health and Human Services (2016) 'Building Community, Building Hope: 2016 prevention resource guide', Available online at https://www.childwelfare.gov/pubPDFs/guide.pdf, Accessed 12/05/2016.

US Government Printing Office (GPO) 'Dep. of Defence Appropriations for fiscal year 2013', Available online at: www.gpo.gov/fdsys/pkg/CHRG-112shrg29104492/html/CHRG-112shrg29104492.htm, Accessed 2/10/ 2013.

Valenzuela, D., & Shrivastava, P. (2008) 'Interview as a method for qualitative research', *Southern Cross University and the Southern Cross Institute of Action Research* (SCIAR). Available online at http://www.public.asu.edu/~kroel/www500/Interview%20Fri.pdf, Accessed 18/02/2016.

Van der Meulen, Nicole, Eun Jo and Stefan Soesanto (2015) 'Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses', *RAND*, Santa Monica, CA: RAND Corporation, 2015. http://www.rand.org/pubs/research_reports/RR1354.html, Accessed 17/01/2016.

Van Eecke & L. Marshall (2015) 'Europe: A new set of rules in the Cybersecurity space', Available online at http://blogs.dlapiper.com/privacymatters/europe-a-new-set-of-rules-in-the-cybersecurity-space/#more-1687, Accessed at 14/12/2015.

Vance, A. (2012) 'Facebook: The Making of 1 Billion Users (04/10/2012)', Bloomberg Business', Available at http://www.bloomberg.com/bw/articles/2012-10-04/facebook-the-making-of-1-billion-users, Accessed 17/13/2013.

Vinocur, N. and Briancon, P. (2015) 'Francois Hollande: We will 'destroy' ISIL (16/11/2015)', *Politico*, Available online at http://www.politico.eu/article/attack-on-paris-francois-hollande-calls-for-un-security-council-meeting/, Accessed 3/12/2015.

Volz, D. (2015) 'U.S., Europe Forge Data-Protection 'Umbrella Agreement' for Terrorism Cases (8/09/2015)', *Government Executive*, Available online at http://www.govexec.com/management/2015/09/us-europe-forge-data-protection-deal-terrorism-cases/120509/, Accessed 11/09/2015.

Walker, C. (2015) 'Cybersecurity Directive: Council announces agreement on main principles – but devil in the detail on scope "still to be discussed" (30/06/2015)', Available at http://datonomy.eu/2015/06/30/cybersecurity-directive-council-announces-agreement-on-main-principles-but-devil-in-the-detail-on-scope-still-to-be-discussed/, Accessed 19/07/2015.

Walt, S. M. (2011) 'The myth of American exceptionalism (11/10/2011)', *Foreign Policy*. Available online at http://foreignpolicy.com/2011/10/11/the-myth-of-american-exceptionalism/, Accessed 24/11/2013.

Ward, S. (2015) 'China admits it has cyber warfare units', https://www.bestvpn.com/blog/15425/china-admits-it-has-cyber-warfare-units/,

Ware, W. H. (1966) 'Future Computer Technology and Its Impact', (No. RAND-P-3279). RAND Corp. Santa Monica CA. http://www.rand.org/content/dam/rand/pubs/papers/2008/P3279.pdf, Accessed 23/03/2014.

Ware, W. H. (1967) 'Security and privacy in computer systems', In *Proceedings of the April 18-20, 1967, Spring Joint Computer Conference* (pp. 279-282). ACM. http://www.rand.org/content/dam/rand/pubs/papers/2005/P3544.pdf, Accessed 20/03/2014.

Ware, W. H. (1970) 'Security controls for computer systems', *Report of Defense Science Board Task Force on Computer Security* (No. RAND/R-609-1). Rand Corp. Santa Monica CA. http://seclab.cs.ucdavis.edu/projects/history/papers/ware70.pdf, Accessed 25/03/2014.

Ware, W. H. (1987) 'Computer security policy issues: from past toward the future', Rand Corp. Santa Monica CA.

Warner, G. (2014) 'Blackshades RAT leads to 97 arrests in 16 countries (22/05/2014)' Cybercrime and doing time, Available online at http://garwarner.blogspot.hu/2014/05/blackshades-rat-leads-to-97-arrests-in.html, Accessed 26/03/2015.

Wei, Wang (2014) 'FBI raids Blackshades RAT Malware Customers in Europe and Australia', *Hacker News*. Available online at http://thehackernews.com/2014/05/fbi-raids-blackshades-rat-malware_16.html, Accessed 11/09/2015.

Weiss, G. W. (1996) *The Farewell Dossier*. Central Intelligence Agency Washington DC Centre for the study of intelligence.

Weiss, M. A. and Archick, K. (2016) 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield (19/05/2016)', *Congressional Research Service*, Library of Congress. Available online at https://www.fas.org/sgp/crs/misc/R44257.pdf, Accessed 19/06/2016.

Weiss, N. E. (2015) 'Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis (3/06/2015)', *Congressional Research Service*, Library of Congress. Available online at https://www.fas.org/sgp/crs/misc/R43821.pdf, Accessed 9/08/2015.

White House (2003) 'The national strategy for The Physical Protection of Critical Infrastructures and Key Assets', Washington, D.C.: White House. Available online at https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf, Accessed 14/02/2013.

White House (2009) 'US Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure', Available online at: www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, Accessed 3/01/2013.

White House (2013a) 'Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (12/12/2013)', By Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. Available online at https://www.whitehouse.gov/sites/default/files/docs/20131212_rg_final_report.pdf, Accessed 18/01/2014.

White House (2013b) 'Presidential Policy Directive - Critical Infrastructure Security and Resilience (12/02/2013)', Office of Press Secretary, Available online at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, Accessed 18/07/2014.

White House (2014) 'Remarks by the President on Review of Signals Intelligence (17/01/2014)', Available online https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence, Accessed 06/07/2015.

White House (2015a) 'Fact Sheet: U.S. – UK Cyber Security cooperation (16/01/2015)', Office of the Press Secretary. Available online at https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation, Accessed 24/04/2015.

White House (2015b) 'President Xi Jinping's State Visit to the United States (25/09/2015)', Office of the Press Secretary. Available online at https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states, Accessed 27/09/2015.

Wikileaks (2008) Secret State 116943, NOFORN, E.O. 12958, *Diplomatic Security Daily*, Public Library of US Diplomacy. Available online at https://wikileaks.org/plusd/cables/08STATE116943_a.html, Accessed 23/09/2015.

Williams, Pete (2014) 'U.S. Charges China With Cyber-Spying on American Firms (19/05/2014)', *NBC News*, Available online at http://www.nbcnews.com/news/us-news/u-s-charges-china-cyber-spying-american-firms-n108706, Accessed 27/08/2014.

Wilson, T. R. (2002) 'Statement Before The Senate Select Committee on Intelligence', available at: www.intelligence.senate.gov/020206/wilson.html, Accessed 23/02/2014.

Woods, A. K. (2015) 'Data Beyond Borders: Mutual legal assistance in the Internet age', *Global Network Initiative*. Available online at https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf, Accessed 29/08/2015.

Wright, S. (1998) An appraisal of technologies for political control. *European Parliament: Scientific and Technologies Options Assessment, Luxembourg*. Available online at https://officinafisica.noblogs.org/files/2012/02/An-Appraisal-of-Technologies-of-Political-Control.pdf, Accessed 24/02/2013.

Yunos, Z. and Ahmad, R., (2014) 'The Application of Qualitative Method in Developing a Cyber Terrorism Framework', *Proceedings of the 2014 International Conference on Economics, Management and Development*. Interlaken, Switzerland February 22-24, 2014.

Zetter, K. (2014) 'Meet MonsterMind, the NSA Bot That Could Wage Cyberwar Autonomously (13/08/2014)', *Wired*. Available online at https://www.wired.com/2014/08/nsa-monstermind-cyberwarfare/, Accessed 19/02/2015.