ЕВРОПЕЙСКИ ПАРЛАМЕНТ PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAIMINT NA hEORPA PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU PARLAMENTUL EUROPEAN
EURÓPSKY PARLAMENT EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

Directorate-General for Internal Policies
Directorate C - Citizens' Rights and Constitutional Affairs

CYBERSECURITY IN THE EUROPEAN UNION AND BEYOND:
Exploring the Threats and Policy Responses

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CYBERSECURITY IN THE EUROPEAN UNION AND BEYOND: EXPLORING THE THREATS AND POLICY RESPONSES

STUDY

Abstract

This study was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee. It sets out to develop a better understanding of the main cybersecurity threats and existing cybersecurity capabilities in the European Union and the United States. The study further examines transnational cooperation and explores perceptions of the effectiveness of the EU response, pinpointing remaining challenges and suggesting avenues for improvement.

This document was requested by the European Parliament's Committee on Justice, Liberty and Home Affairs.

AUTHORS

Dr Nicole van der Meulen (Analyst, RAND Europe, Cambridge Office)
Eun A Jo (Intern, RAND Europe, Cambridge Office)
Stefan Soesanto (Research Assistant, RAND Europe, Brussels Office)

RESPONSIBLE ADMINISTRATOR

Mr Darren Neville
Policy Department Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its monthly newsletter please write to: poldep-citizens@europarl.europa.eu

Manuscript completed in September 2015.

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

ACKNOWLEDGEMENT

The authors would like to express their gratitude to the experts and practitioners whose interviews and/or written contributions considerably enriched this study. We are also grateful to RAND Europe's Sarah Grand-Clement and Sonja Thebes for their research support and to RAND Europe's Susanne Sondergaard, Emma Disley and Paul Cornish, as well as RAND Corporation's Lily Ablon for their constructive feedback.

CONTENTS

LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
ACSC	Australian Cyber Security Centre
AES	Advanced Encryption Standard
ALM	Avid Life Media
APT	Advanced Persistent Threats
BBC	British Broadcasting Corporation
BEK	Blackhole Exploit Kit
BKA	Bundeskriminalamt (German Federal Criminal Police Office)
BSA	Business Software Alliance
BSI	Bundesamt fuer Sicherheit in der Informationstechnik (German Federal Office for Information Security)
C3	US Immigration and Customs Enforcement (ICE) Cyber Crimes Center
C&C	Command and Control
CCDCOE	Cooperative Cyber-Defence Centre of Excellence
CCIPS	Computer Crime and Intellectual Property Section
CDM	Continuous Diagnostics and Mitigation
CEPOL	European Police College
CERTs	Computer Emergency Response Teams
CERT-EU	Computer Emergency Response Team – European Union
CFAA	Computer Fraud and Abuse Act
CFSP	Common Foreign and Security Policy
CIA	Central Intelligence Agency
CISA	Cybersecurity Information Sharing Act
CISCP	Cyber Information Sharing and Collaboration Program
CJEU	Court of Justice of the European Union
CMF	Cyber Mission Force
COE	Council of Europe
CRISP	Cybersecurity Risk Information Sharing Program
CSAN	Netherlands Cyber Security Threat Assessment
CSDP	Common Security and Defence Policy
CSIRTs	Computer Security Incident Response Teams
CS&C	Office of Cybersecurity and Communications
CTIIC	Cyber Threat Intelligence Integration Center
CTO	Chief Technology Officer

DBIR	Data Breach Investigations Report
DD4BC	Distributed Denial-of-Service for BitCoin
DDoS	Distributed Denial-of-Service
DGA	Domain Generating Algorithm
DHS	US Department of Homeland Security
DLoDs	Defence Lines of Development
DNI	US Director of National Intelligence
DNS	Domain Name System
DoD	US Department of Defense
DoJ	US Department of Justice
DRIPA	Data Retention and Investigatory Powers Act
EC3	European Cyber Crime Centre
EC3AA	European Cyber Crime Centre Academic Advisory Network
ECB	European Central Bank
ECJ	European Court of Justice
ECS	Enhanced Cybersecurity Services
ECTEG	European Cybercrime Training and Education Group
EDA	European Defence Agency
EEAS	European External Action Service
EFF	Electronic Frontier Foundation
EJN	European Judicial Network
EMAS	Europol Malware Analysis System
EMEA	Europe, Middle East and Africa
EMPACT	European Multidisciplinary Platform Against Criminal Threats
ENISA	European Network and Information Security Agency
EO	Executive Order
EP	European Parliament
ESS	Office of the Special Prosecutor (Iceland)
ETL	ENISA Threat Landscape
EU	European Union
EUCTF	European Union Cybercrime Task Force
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FHQ	Force Headquarters
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
HSI	Homeland Security Investigations
HSSAI	Homeland Security Studies and Analysis Institute
IC3	Internet Crime Complaint Center
ICE	Immigration Customs Enforcement
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IOC	Incident of Compromise
iOCTA	Internet Organised Crime Threat Assessment (Europol)
IoT	Internet of Things
IP	Internet Protocol
IRU	Internet Referral Unit
ISACs	Information Sharing and Analysis Centers
ISAO	Information Sharing and Analysis Organisation
ISO	International Standards Organisation
ISP	Internet Service Provider
IT	Information Technology
ITOM	Illegal Trade and Online Marketplaces
J-CAT	Joint Cybercrime Action Taskforce
JITs	Joint Investigation Teams
LRH	Reykjavik Metropolitan Police
MaaS	Malware-as-a-Service
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
mTAN	Mobile Transaction Authentication Number
NACHA	US National Automated Clearing House Association
NATO	North Atlantic Treaty Organization
NCA	UK National Crime Agency
NCC	US National Coordinating Center for Telecommunications
NCCIC	US National Cybersecurity and Communications Integration Center
NCIJTF	US National Cyber Investigative Joint Task Force
NCKB	Czech National Security Centre
NCPAA	US National Cybersecurity Protection Advancement Act
NCSC	Dutch National Cyber Security Centre
NDAA	US National Defence Authorization Act

NHTCU	Dutch National High Tech Crime Unit
NIS	Network and Information Security
NIST	US National Institute of Standards and Technology
NMS-CO	US National Military Strategy for Cyberspace Operations
NCCIC	US National Cybersecurity and Communications Integration Center
NSA	US National Security Agency
OECD	Organisation for Economic Cooperation and Development
OHQ	Operational Headquarters
OIG	Office of the Inspector General
OLAF	European Anti-Fraud Office
OM	Openbaar Ministerie (Dutch Public Prosecutor's Office)
OMB	Office of Management and Budget
OPM	Office of Personnel Management
P2P	Peer-to-Peer
PCNA	Protecting Cyber Networks Act
PDD	Presidential Decision Directive
PII	Personal Identifying Information
PoS	Point-of-Sale Malware
RAT	Remote Access Tool
RCS	Remote Control System
RLS	National Commission of the Icelandic Police
TF-CSIRT	Task Force Computer - Security and Incident Response Team
TOR	The Onion Router
ToT	Training of Trainers
TTPs	Tactics, Technologies and Procedures
UK	United Kingdom
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
US	United States
USCYBERCOM	United States Cyber Command
US-CERT	United States - Computer Emergency Response Team
USB	Universal Serial Bus
USSS	United States Secret Service

LIST OF FIGURES AND TABLES

EXECUTIVE SUMMARY

The European Commission published the European Union Cyber Security Strategy along with the accompanying proposal for a Network and Information Security (NIS) Directive in 2013. Since the proposal was published, the cybersecurity landscape has continued to evolve, leading to questions regarding the nature and seriousness of the cyberthreats faced by the European Union (EU), the capabilities of Member States to manage these threats and respond to incidents, and the effectiveness of these capabilities. At the time of writing, discussions about the content and scope of the proposed NIS Directive are continuing.

This study of cybersecurity threats in the EU was commissioned by the European Parliament (EP). It has five objectives:

1. To identify key cyberthreats facing the EU and the challenges associated with their identification.
2. To identify the main cybersecurity capabilities in the EU.
3. To identify the main cybersecurity capabilities in the United States (US).
4. To assess the current state of transnational cooperation.
5. To explore perceptions of the effectiveness of the current EU response.

Defining cybersecurity

Any study of cybersecurity must reflect on the challenges introduced by the different meanings of the term. There is no consensus on a standard or universally accepted definition of cybersecurity. The term cybersecurity has roots in information security but is now used to refer to a broader range of issues, linked to national security. The observation that cybersecurity means different things to different people is not without its consequences. How the issue is framed influences what constitutes a threat as well as what counter-measures are needed and justified.

Mapping cybersecurity threats

The study team's analysis of six threat assessments[1] and an existing meta-analysis carried about by Gehem et al. (2015) highlight the difficulty with systematically comparing threat assessments and gauging the reliability of data and findings on the basis of which threat assessments are conducted. The challenge rests in part in the absence of a commonly accepted definition of what constitutes a threat and the variation in the methodology and metrics used for threat assessments. Moreover, some threat assessments reference or are based on other threat assessments, rather than original sources, leading to potential duplication of findings and lack of clarity about the evidence underlying threat assessments. As a result, there is no clearly established framework to classify and map threats.

The study team created a framework for mapping threats. The framework distinguishes:

- **Threat actors:** states, profit-driven cybercriminals, and hacktivists and extremists.
- **Threat tools:** malware and its variants, such as (banking) Trojans, ransomware, point-of-sale malware, botnets and exploits.
- **Threat types:** unauthorised access, destruction, disclosure, modification of information and denial of service.

[1] (ACSC: Threat Report; BSI: State of IT Security Germany; ENISA: Threat Landscape (ETL); Europol: Internet Organised Crime Threat Assessment (iOCTA); NCSC: Cyber Security Threat Assessment the Netherlands (CSAN); Verizon: Data Breach Investigations Report (DBIR).

The mapping of the cyberthreat landscape through the review of the six threat assessments was complemented by a discussion on the varying perceptions of the severity of threats and the concept of 'threat inflation'.

Cybersecurity capabilities in the EU

To respond to the evolving threat in the area of cybersecurity, the EU has aimed to provide an overarching response through the publication of the EU Cyber Security Strategy together with the proposed NIS Directive. The Strategy identifies five objectives including:

1. Achieving cyberresilience.
2. Drastically reducing cybercrime.
3. Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP).
4. Developing the industrial and technological resources for cybersecurity.
5. Establishing a coherent international cyberspace policy for the EU and promote core EU values.

This study focuses on providing a descriptive overview of capabilities for the first three objectives. Capabilities for the purposes of this study have been operationalised as institutional structures, such as agencies and departments.

- In the area of cyberresilience, the European Network and Information Security Agency (ENISA) is the primary player at the EU level. ENISA is tasked with addressing the existing fragmentation in the European approach to cybersecurity, namely by bridging the capability gaps of its Member States. In the cybercrime domain, the European Cyber Crime Centre (EC3) serves as a European cybercrime platform. Besides combatting cybercrime, EC3 also gathers cyberintelligence and serves as an intermediary among various stakeholders, such as law enforcement authorities, Computer Emergency Response Teams (CERTs), industry and academia.
- In the area of cyberdefence, the European Defence Agency (EDA) supports the capability development necessary to implement the Strategy. Its most apparent activities remain in research and development and designing a common crisis response platform. Given that foreign and defence policies have conventionally been areas of domestic competence, it is understandable that EU-wide cyberdefence capabilities have developed at a different pace compared to the other two objectives, cyberresilience and cybercrime.

Cybersecurity capabilities in the US

Cybercapabilities in the US are challenging to map in a comprehensive manner. The tendency to layer initiatives and agencies makes navigating the different components difficult. For the purposes of a high-level comparison with the EU cyber capabilities, the study focuses on key institutional players and their roles in relation to three strategic priorities: cyberresilience, cybercrime and cyberdefence.

- In the area of cyberresilience, the Department of Homeland Security (DHS) is the formal leader. The DHS is responsible for securing federal civilian government networks, protecting critical infrastructure and responding to cyberthreats.
- In the area of cybercrime, the US has not designated any lead investigative agency. Instead, numerous federal law enforcement agencies combat cybercrime in their own capacity. These include the US Secret Service (USSS) and the US Immigration and Customs Enforcement (ICE) Cyber Crimes Center, which are

both agencies within the DHS. The Federal Bureau of Investigation (FBI)'s cyberdivision is also involved.

- In cyberdefence, the Department of Defence (DoD) plays a leading role. It is readily apparent from the DoD's multiple publications that the US has become more open about its capabilities and willing to name its adversaries. The DoD is also increasingly encompassing in its response to cyberthreats over time, investing in both defensive as well as offensive cybercapabilities, as detailed in its cyberdefence strategy published in April 2015. Commentators note that deterrence is a key characteristic of the US cyberdefence strategy.

Transnational cooperation

The necessity to engage in transnational cooperation to counter the complex challenge posed by cybercrime is widely recognised both inside and outside the EU. Transnational cooperation exists at both the strategic and the operational level. The EU-US Working Group on Cybersecurity and Cybercrime is an example of strategic cooperation and is the first transatlantic dialogue to tackle common challenges in the area of cybercrime and cybersecurity. On an operational level, transnational cooperation has manifested through a range of activities, from botnet takedown to disruption of underground forums.

Challenges, however, remain in the area of combatting cybercrime as identified by the study team through the interviews. Mutual Legal Assistance Treaties (MLATs) are widely regarded as outdated and obstacles to effective and timely information sharing. Further, the importance of acquiring data for investigations is debated among law enforcement agencies and civil society groups. Deconfliction – avoiding the duplication or conflict of efforts – is another challenge. Due to the involvement of various stakeholders, cooperation is essential to avoid potentially disrupting others' efforts. The draft Europol Regulation contains provisions that interviewees have reported could complicate the attainment of information from the private sector, possibly obstructing future operations.[2]

Effectiveness of the EU response

Ideally, capabilities respond directly to threats and the effectiveness of the EU response can be measured by noticeable changes in the threat landscape. However, such an assessment is not feasible; there is not enough information available in the public domain and measurement problems persist. Moreover, the EU response is still very much in development and geared towards addressing fragmentation in its approach to cybersecurity, as well as the approach taken by the 28 Member States. This consists of harmonising strategies and standards and coordinating regulatory interventions, as well as facilitating (or more precisely, requiring) information sharing and gap closures between Member States. Due to the inherently relative nature of cybersecurity and the challenges associated with attaining cyberresilience, it is difficult to state whether the new initiatives have been successful. Given these challenges to measuring effectiveness, the study team explored perceptions about the effectiveness of the EU response based on existing commentary and supplemented with interviewees' responses.

[2] European Parliament. 2014b. *Legislative resolution of 25 February 2014 on the proposal for a regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA*. P7_TA(2014)0121 (COM(2013)0173 – C7-0094/2013 – 2013/0091(COD)). As of 12 October 2015: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0121&language=EN&ring=A7-2014-0096

The first key finding in relation to the perceived effectiveness of the EU response is that while there is still fragmentation, there is also discernible improvement. Particularly noteworthy is the strategic cooperation agreement between ENISA and EC3, which aims to facilitate closer cooperation and the exchange of expertise. However, questions remain about fragmentation, especially with respect to the proposed NIS Directive. Various points of dissension remain as the trilogue negotiations between the European Commission, European Parliament and the Council of the European Union continue. Moreover, fragmentation is notable not only in terms of operational capabilities but also in terms of Member States' understanding of the cyberdomain. Bridging these gaps will therefore require technical support as well as strategic guidance.

The second finding is that differences in opinion persist as to whether the overall approach to cybersecurity should be voluntary and informal or mandatory and formal. For example, the CERT community, which has conventionally relied on voluntary participation and cooperation between private and public entities, appears less willing to move to a system in which information sharing is mandatory. In contrast, other security agencies favour law enforcement and support more stringent requirements, for instance in information sharing, as they believe voluntary reporting has failed.

Third, as the new approach proposed through the Strategy and the draft NIS Directive is largely regulatory in nature, the issue of scope – in terms of the entities formally included as having a role in cybersecurity – is heightened and contested. One issue is whether Internet service providers (ISPs) should be included. These scoping challenges are likely to exacerbate existing contentions surrounding the NIS Directive and call into question whether the present regulatory approach is appropriate to secure European cyberspace.

Policy options

Based on this study's findings the research team suggests the following policy options for the European Parliament's consideration in terms of EU action on cybersecurity. Each option is elaborated in the Conclusion.

1. **Encourage ENISA, EC3 and others involved in European cyberthreat assessments to investigate further harmonisation of threat assessments, which can effectively incorporate information from Member States and other EU agencies and provide clearer indications of the evidence base for the assessment.** This recommendation follows from the findings from the review of threat assessments undertaken for this study.
2. **Make use of existing structures as much as possible.** One of the concerns identified by the study team – from a review of existing literature and in interviews with experts – was the tendency of the Commission to develop new structures and exclude existing initiatives and agencies.
3. **Consider reinserting law enforcement in the Network and Information Security (NIS) Directive.** The attempt to overcome fragmentation at the EU level is hampered by the exclusion of law enforcement from provisions in the proposed NIS Directive.
4. **Ensure Europol has speedy and more direct access to information from the private sector**. Speedy access to relevant information from the private sector is essential for Europol to combat transnational cybercrime. There is potential for this access to be hindered by having to go through the Member States, which may reduce the effectiveness of Europol's operations, especially as Europol cooperates with partners at the transnational level.

5. **Assess what capability gaps actually exist between the Member States and measure progress.** Despite the claims about gaps between Member States, our research suggests that there is very little empirical evidence to indicate which States are more advanced than others and in what areas. To improve this situation and to develop a better understanding of these gaps, ranking Member States and identifying areas of improvement could be made more explicit.

1 INTRODUCTION

Cybersecurity incidents – most notably breaches of data security – make headlines daily in the media. Both 2013[3] and 2014[4] have been labelled years of megabreaches. Verizon's 2015 Data Breach Investigations Report (DBIR) recorded 79,790 security incidents in 2014, across 61 countries.[5] This includes 2,122 confirmed data breaches. To put things into perspective, 1,023,108,207 recorded breaches originated from just 1,541 of these incidents, marking a 78 per cent increase in recorded compromised personal data since 2013.[6]

According to the 2014 Cost of Data Breach Study by the Ponemon Institute, the average cost of responding to a data breach for a company rose to $3.5 million, a 15 per cent increase on the previous year.[7] All of this demonstrates that the year 2014 was characterised by large-scale breaches of high-profile organisations – the likes of eBay, Adobe and J.P. Morgan.

The rising number of security breaches (and the seriously negative perception of the security of cyberspace they have created) led to substantial increases in the information technology (IT) security budgets of governments, corporations and individuals.[8] Cybersecurity has become a mainstream topic of discussion: 'The year 2014 saw the term "data breach" become part of the broader public vernacular with *The New York Times* devoting more than 700 articles related to data breaches, versus fewer than 125 the previous year.'[9]

While more than two years have passed since the *Guardian* broke its first news story on the mass surveillance carried out by the United States (US) National Security Agency (NSA), the ripples of Edward Snowden's revelations resonate to this day. In particular, as the European Parliament (EP) noted, transatlantic trust has been 'profoundly shaken' since. In the digital era, states can be allies in the fight against cybercrime but competitors in the area of national cybersecurity. This potential conflict of interest or paradox – both between as well as within states – introduces many challenges in addition to the inherent complexity introduced through cyberinsecurity. These challenges require answers, especially as society's dependence on digital technologies and digital infrastructure continues to grow. To provide such answers, a better understanding of a number of facets of the cybersecurity landscape is required.

1.1 Cybersecurity in the EU

The European Union (EU) recognises the importance of cybersecurity, as expressed through its publication of the EU Cyber Security Strategy in February 2013 and the

[3] Hattem, Julian. 2014. 'Report calls 2013 year of the mega breach.' *The Hill*, August 4. As of 12 October 2015: http://thehill.com/policy/technology/202913-report-calls-2013-year-of-the-mega-breach
[4] Ponemon Institute. 2015. 2014: A year of mega breaches. As of 12 October 2015: http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf
[5] The report consolidates data from 70 different organisations in 61 countries. See: Verizon. 2015. 2015 Data Breach Investigations Report. As of 12 October 2015: http://www.verizonenterprise.com/DBIR/2015/
[6] Kharpal, Arjun. 2015. 'Year of the hack? A billion records compromised in 2014.' *CNBC*, February 12. As of 12 October 2015: http://www.cnbc.com/2015/02/12/year-of-the-hack-a-billion-records-compromised-in-2014.html
[7] Ponemon Institute. 2014. 'Ponemon Institute releases 2014 Cost of Data Breach: Global Analysis.' *Ponemon Institute Blog*, August 26. As of 12 October 2015: http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis. See also: Jardine, Eric. 2015. Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime. *Global Commission on Internet Governance*, No. 16. As of 12 October 2015: https://www.cigionline.org/sites/default/files/no16_web_0.pdf
[8] Jardine 2015.
[9] Verizon 2015.

accompanying proposal for a Network and Information Security (NIS) Directive. Since the publication of these documents, cybersecurity has continued to evolve and become an increasingly complex topic of public policy.

1.2 Objectives of the study

The European Parliament (EP) Committee on Civil Liberties, Justice and Home Affairs (LIBE) requested a study of cybersecurity addressing the following five objectives:

- The first objective is to provide an overview of the main threats facing the EU. This will allow the LIBE Committee to develop an understanding of the most urgent threats and subsequently to determine how these relate to existing as well as proposed capabilities and their effectiveness.
- The second objective is to provide an overview of the cybersecurity capabilities within the EU. For the purposes of this study, cybersecurity capabilities have been translated into the main agencies or departments that exist within the EU and the role they play in cybersecurity. This will be discussed in tandem with relevant existing legislation or legislative proposals.
- To enhance policy learning and to understand how cybersecurity is approached in a 'comparable' region, the third objective of the study is to provide an overview of cybersecurity capabilities in the US. For comparative purposes, the chapter on the US will follow the same structure as the chapter on the EU.
- The fourth objective is to provide an insight into transnational cooperation with the aim of identifying remaining challenges and areas for improvement.
- The fifth objective is to provide an overview of the response offered by the EU or to capture the impression of its effectiveness.

1.3 What is cybersecurity?

Before embarking on the analysis of cybersecurity threats and capabilities, the meaning of the concept of cybersecurity must be established. Although this may appear to be a straightforward exercise, it is actually a challenging endeavour. There is consensus that there is no standard or universally accepted definition of cybersecurity.[10] As indicated on the website of the Cooperative Cyber Defence Centre of Excellence (CCDCOE) at the North Atlantic Treaty Organisation (NATO): 'There are no common definitions for Cyber terms – they are understood to mean different things by different nations/organisations, despite prevalence in mainstream media and in national and international organisational statements.'[11] Choucri et al. echo this lack of an agreed understanding of the concept and also emphasise how the lack of consensus about how it is spelled (for example, cybersecurity, cyber security, cyber-security) can be a serious impediment to developing theory and policy, not least because these variations in spelling complicate the ability to capture all relevant knowledge on the topic.[12]

[10] See also: Silva, Karine E. 2013. 'Europe's fragmented approach towards cyber security.' *Internet Policy Review* 2(4). As of 12 October 2015: http://policyreview.info/articles/analysis/europes-fragmented-approach-towards-cyber-security

[11] North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2015. 'Cyber definitions.' As of 12 October 2015: https://ccdcoe.org/cyber-definitions.html

[12] Choucri, Nazli, Gihan Daw Elbait & Stuart Madnick. 2012. *What is Cybersecurity? Explorations in Automated Knowledge Generation*. As of 12 October 2015: http://ecir.mit.edu/images/stories/Madnick%20et%20al%20Comparison%20Paper%20for%20ECIR%20workshop%20-%20Fig%201%20also%20FIXED%20v2.pdf

Besides a lack of a common meaning, the concept of cybersecurity is controversial in itself. Herr & Friedman (2015) capture best the current state of affairs: 'Cybersecurity is an often abused and much misused term that was once intended to describe and now serves better to confuse.'[13] For those in the information security community, the uptake of the term cybersecurity is an undesirable development brought about by policymakers who have little knowledge of the subject matter. As Cornish et al. put it: 'Where cyberspace and national security are concerned, there is a disconnect between technology and public policy […] Science and technology should be more closely informed by public policy, while a technologically informed political leadership should be better placed to meet the cybersecurity challenge.'[14] 'Cyber' is frequently referred to as 'Washington parlance'. In 2008, Edward Felten, Professor of Computer Science and Public Affairs at Princeton University, reflected on the evolution of cybersecurity as a term in policy communication.[15] He indicated that beyond government the terms 'information security', 'network security' or 'computer security' are more dominant and that the introduction of a more militaristic approach to information security transformed the concept to cybersecurity, and often just 'cyber'.

Resistance to use of the term cybersecurity, as opposed to information security, appears to originate largely from the transformation of information security into a national security domain. As the Organisation for Economic Cooperation and Development (OECD) notes, the lack of specificity of the term, especially in connection to its transformation into a national security concern, may lead to 'drastic solutions' like network monitoring as opposed to 'practical solutions' that are more respectful of citizens' rights.[16]

The fact that cybersecurity means different things to different people has definite consequences; the way in which the issue is framed influences what constitutes a threat as well as what measures are needed and justified.

Broerders describes how the engineering approach of Computer Emergency Response Teams (CERTs), focused primarily on keeping a network 'healthy', and that this created difficulties with the national security stakeholders, such as intelligence services and military departments, with whom CERTs cooperated at international level. The convergence of these different perspectives on security is undesirable, according to Broeders et al., because the partial interest of national security clashes with the collective interest of security of the network as a whole. He therefore suggests:

> *To clearly differentiate at the national and international level between Internet security (security of the Internet infrastructure) and national security (security through the Internet) and have separate parties address these different forms.*[17]

---

[13] Herr, Trey & Allan Friedman. 2015. 'Redefining Cybersecurity.' *The American Foreign Policy Council Defense Technology Program Brief*, January 22. As of 12 October 2015: http://www.afpc.org/publication_listings/viewPolicyPaper/2664

[14] Cornish, Paul, Rex Hughes & David Livingstone. 2009. *Cyberspace and the National Security of the UK*. Chatham House. As of 12 October 2015: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r0309cyberspace.pdf

[15] Felten, Ed. 2008. 'What's the Cyber in Cyber-security?' Freedom to Tinker, July 24. As of 12 October 2015: https://freedom-to-tinker.com/blog/felten/whats-cyber-cyber-security/

[16] Brantly, Aaron F. 2014. 'The Cyber Losers.' *Democracy and Security* 10(2): 132-155

[17] Broeders, Dennis. 2015. *The Public Core of the Internet: An International Agenda for Internet Governance*. WRR Scientific Council for Government Policy, Policy Brief 2. As of 12 October 2015: http://www.wrr.nl/fileadmin/en/publicaties/PDF-WRR-Policy_Briefs/WRR_Policy_Brief__2015__The_Public_Core_of_the_Internet.pdf

Dunn Cavelty previously identified similar concerns.[18] Levin & Goodrick frame the issue in terms of policy arenas:

> *The more countries focus on their cybersecurity from cyberwar, the more they do that at the expense of cooperation on cybercrime. Worries of cyberwar cause countries to align and retrench in their traditional international blocs, at the expense of international treaties that attempt to foster new forms of cooperation against cybercrime.*[19]

The way in which cybersecurity is defined and subsequently framed and approached is of paramount importance to capability development and effectiveness, as well as to threat assessments. The lack of a commonly agreed definition complicates discussions and the involvement of different actors with distinct security interests may lead to potential conflicts of interest.

These challenges do not provide a sufficiently concrete understanding of what is meant by cybersecurity. They merely showcase the complexity of the subject due to the involvement of a range of stakeholders with distinct and often conflicting interests. This note of caution is a leitmotif of this study and should extend to any type of policy introduced under the broad heading of cybersecurity. After all, security for one – in cyberspace and elsewhere – may be insecurity for another.

As a final note, it is essential to reflect on the terminology used within the EU. While the EU has had a cybersecurity strategy since 2013, the principal piece of legislation in this area at the EU level is the proposed Network and Information Security (NIS) directive. It may be that these terms are considered interchangeable within the EU. However, to avoid uncertainty, confusion and even controversy, a more exact and consistent use of language by the EU would without doubt benefit productive debate and rigorous analysis.

1.4 Methodology

To carry out this study, the research team employed the following data collection and research approaches:

- A review of six key threat assessments.[20]
- A targeted review of academic research and literature and media reports on cyberthreats and attacks.
- Interviews with officials in the European Cyber Crime Centre (EC3), the Federal Bureau of Investigations (FBI), the United Kingdom (UK) National Crime Agency (NCA), the Assistant to the Dutch Desk for the Netherlands at Eurojust, the Reykjavik Metropolitan Police (LRH), the Icelandic Special Prosecutor Office (ESS) and the National Commission of the Icelandic Police (RLS).
- Development of case studies of instances of transnational cooperation, based on publicly available information.

[18] Dunn Cavelty, Myriam. 2014. 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities.' *Science and Engineering Ethics* 20(3): 701-715

[19] Levin, Avner & Paul Goodrick. 2013. 'From cybercrime to cyberwar? The international policy shift and its implications for Canada.' *Canadian Foreign Policy Journal* 19(2): 128

[20] (1) ACSC: Threat Report; (2) BSI: State of IT Security Germany; (3) ENISA: Threat Landscape (ETL); (4) Europol: Internet Organised Crime Threat Assessment (iOCTA); (5) NCSC: Cyber Security Assessment the Netherlands (CSAN-4); (6) Verizon: Data Breach Investigations Report (DBIR).

While each chapter relies primarily on desk-based research, where required and possible it was supplemented by interviews. Table 1 provides a broad overview of methods used for investigating each objective of the study (for more detail, see the Annex).

Table 1. Methodology

Objective	Methodology
1. To identify key cyberthreats facing the EU	Desk-based research involving a review of six key threat assessments and an existing meta-analysis
2. To identify main cybersecurity capabilities in the EU	Desk-based research using publicly available literature such as official documents and commentaries
3. To identify main cybersecurity capabilities in the US	Desk-based research using publicly available literature such as official documents and commentaries
4. To assess the current state of transnational cooperation	Desk-based research with a focus on two case studies, supplemented by interviews
5. To explore perceptions as to the effectiveness of the current EU response	Desk-based research using publicly available literature, supplemented by interviews

Source: RAND Europe study team

1.5 Limitations of the study

This study has several limitations. First, in relation to the fourth research question, looking at the effectiveness of the EU response, findings are based on a very small number of interviews, which restricts the representative character of the views. Due to limited availability over the summer and the tight timeframe in which the research was conducted, the study team was unable to interview as many individuals within the domain of cybersecurity in the EU as might be considered desirable for the objectives of this study. As a result, most of the information about effectiveness comes from the literature and other documents that may be able to provide only a partial story.

This study collected information from news sources because, given the rapid pace of development in the cybersecurity field, they are often the only source on recent development. However, news sources may provide incomplete accounts and there are questions about their accuracy.

The third limitation considers the sensitive nature of cybersecurity: information about threats, capabilities or other features remains confidential and is not in the public domain. As a result, a comprehensive overview of all elements is not possible based on the publicly available sources on which this study relied.

The fourth limitation relates to the selection of six threat assessments to review to answer the first research question. These were selected on the basis of their geographic coverage as well as the reputation of the authoring organisations; however, given the vast number of threat assessments that have been published in Europe, the study team recognises that relying on only six has some limitations. Also in relation to the first objective, and as explained further in Chapter 2, there are questions about the evidence bases underlying existing threat assessments on which this study has based the overview of threats facing the EU.

1.6 Structure of the report

This report begins in Chapter 2 with a discussion of cybersecurity threats. Chapter 3 focuses on cybersecurity capabilities in the EU along three key objectives of the EU Cyber Security Strategy, namely cyberresilience, cybercrime and cyberdefence. Chapter 4 provides an overview of cybersecurity capabilities in the US and uses the same organising framework as for the EU. Chapter 5 discusses the effectiveness of the EU response to cybersecurity challenges. Chapter 6 provides a number of case studies of transnational cooperation to illustrate how such cooperation and coordination work in practice and potential challenges identified by interviewees. Finally, Chapter 7 reflects on all the preceding chapters and provides a conclusion to the study, followed by a succinct list of policy recommendations in Chapter 8.

2 MAPPING GLOBAL CYBERSECURITY THREATS: PATTERNS AND CHALLENGES

KEY FINDINGS

- The empirical basis of publicly available threat assessments is often unclear and could be improved with a more robust framework and evidence base.
- Comparison of threat assessments is difficult due to different definitions, metrics, approaches and overlap.
- A review of six threat assessments suggests that among the various threat actors, states and cybercriminals are thought to pose the highest risk.
- There is a view across a number of threat assessments that cybercriminals have become professionalised allowing for the 'industrialisation of cybercrime' and a lower entry threshold.
- Malware is a part of nearly every security incident and continues to proliferate.
- Within the available literature, the perceived level of threat in the area of cybersecurity is varied; in particular, when indicators are expressed in proportion to the growing size of the Internet, the level of security in cyberspace appears better than often portrayed.

2.1 Introduction

To understand what types of cybersecurity capabilities are needed, organisations – in both the public and the private sector – carry out cybersecurity threat assessments. The European Union Cyber Security Strategy (the Strategy) acknowledges and emphasises the importance of threats in the cybersecurity sphere.

This chapter has two objectives. The first is to elaborate on the challenges associated with systematically comparing existing threat assessments due to differences in perspectives on what constitutes a threat and in the underlying methodology of data gathering for the assessments. Moreover, existing threat assessments often rely on each other, which leads to duplication and potential overemphasis of one type of threat over another. Understanding these limitations of existing threat assessments will provide the European Parliament (EP) with the tools to evaluate critically existing threat analyses and recommend improvements to the way in which threat assessments are carried out by EU institutions.

The second objective is to identify threat actors, threat tools and threats, based on a review of six selected threat assessments, and to reflect on how the threat landscape is evolving. This chapter does not systematically review these six threat assessments because of the limitations identified; neither does it assess the importance of each threat, tool, or actor relative to each other or over time. Rather, it provides a descriptive overview of these threat components, supplemented with a brief discussion of varied perceptions about their relative importance provided by the existing literature.

2.2 What is a threat?

There is no universal or standard understanding of the concept of a threat. Hans Gunter Brauch provides an extensive overview of the related concepts of security threats,

challenges, vulnerabilities and risks.[21] According to Brauch, 'threat' is used as both a political term and a scientific concept. He cites various dictionary definitions and concludes that 'the common use of the term' in both British and American English maintains multiple meanings. With respect to threat as a scientific concept, he acknowledges that 'threat' often remains undefined in social science dictionaries.

From a more practical perspective, the International Standards Organisation (ISO) defines a threat as:

> *A potential event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organisation or system.*[22]

On the other hand, the National Institute of Standards and Technology (NIST) in the United States (US) defines a threat as:

> *Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.*[23]

Two aspects of this NIST definition are important for the purposes of this study. The first is that the inclusion of 'circumstance' broadens the definition to include (arguably) threat tools and vulnerabilities, which can broaden and potentially confuse a threat overview. The second aspect is the inclusion of threat types, which is an advantage of this definition. By mentioning 'unauthorised access, destruction, disclosure, modification of information and/or denial of service', the definition identifies actions that can be taken against information as well as information systems. This forms the core of types of threat to cybersecurity.

For the purposes of this study, we use the ISO definition, which limits threat to a potential event; yet, we complement this definition with the NIST categorisation of threats. Circumstances that may facilitate the occurrence of such an event are enabling or facilitating factors, such as threat tools. This operationalisation of different key concepts is recommended, as it can assist in establishing a clearer framework for future threat assessments and establishes a more robust categorisation mechanism.

2.3 Challenges with existing threat assessments

Before moving on to the analysis of existing threat assessments, a brief reflection on the challenges associated with them is warranted, especially with a view to providing the EP with the tools to evaluate critically available data on threats. The main challenge stems from the absence of a commonly agreed definition (see Section 2.2). This absence prevents the establishment of a universally accepted categorisation system for threats and leads to variability in what is included in threat assessments.

[21] Brauch, Hans Gunter. 2011. 'Concepts of security threats, challenges, vulnerabilities, and risks.' In: Brauch et al. 2011. *Coping with Global Environmental Change, Disasters, and Security*. Berlin: Springer-Verlag
[22] Praxiom Research Group Limited. 2013. 'Plain English ISO IEC 27000 2014 Information Security Definitions. 2014.' As of 12 October 2015: http://www.praxiom.com/iso-27000-definitions.htm
[23] National Institute of Standards and Technology (NIST). 2006. *Minimum security requirements for federal information and information systems*. FIPS PUB, 9 March. As of 12 October 2015: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

The literature also reflects on the challenges of existing threat assessments. Gehem et al. conducted a meta-analysis of 70 cybersecurity threat analysis reports and studies.[24] They observe how the reports develop a rather fragmented overview, due to multiple causes. First, some reports focus on all potential cybersecurity threats whereas others focus specifically on particular types of threat. Second, the focus of reports ranges from global, including all public and private sectors, to selected countries or sectors. Third, the methodologies used by existing reports differ and often lack transparency. This makes comparisons between results difficult and also influences the quality of the data.[25] As Gehem et al. summarise:

> *One of the main observations of our study is that the range of estimates in the examined investigations is so wide, even experts find it difficult to separate the wheat from the chaff*.[26]

As a result, the development of a comprehensive threat overview is currently still a challenge, especially if such an overview must take into account the diversity of actors – both in terms of victims or targets as well as perpetrators or threat actors. This goes back to the previously identified challenge of how cybersecurity is defined by different stakeholders with divergent interests (see Sections 1.3 and 2.2) as well as the understanding of what constitutes a threat (see Section 2.2). Challenges associated with existing approaches to threat assessments have also previously been recognised by the European Network and Information Security Agency (ENISA).[27]

Another issue identified in our analysis of a limited sample of threat assessments is duplication, since various documents rely on information provided by other threat assessments. The ENISA Threat Landscape (ETL) is an example: the report incorporates data from the Verizon Data Breach Investigations Report (DBIR) and from the Cyber Security Assessment Netherlands (CSAN). This makes counting the frequency of times a particular threat or tool is mentioned an inadequate way of identifying the urgency of a threat. Moreover, such a methodological approach can also overemphasise certain threats, especially when the basis for the original identification of a particular threat is absent or is duplicated without a critical evaluation.

2.4 Mapping the cyberthreat landscape

For the purposes of this study, the project team has limited its evaluation to six existing threat assessments. The selection of these assessments was based on a number of criteria. The first criterion was the authoring organisation. Private sector reports, i.e. those that did not involve public sector or academic stakeholders, were excluded. The study team focused on reports published either by public sector stakeholders, such as EU institutions and Member States, or the private sector in cooperation with public sector stakeholders, such as the Verizon DBIR. A specific emphasis was placed on reports considered to be authoritative, either because of a long history of the report, or because of the authoring organisation, or both. The second criterion was date of publication. Only reports published either in or after 2014 were included in the analysis. The third was

[24] Gehem et al. 2015. *Assessing cyber security – A meta-analysis of threats, trends, and responses to cyber attacks*. The Hague: The Hague Center for Strategic Studies. As of 13 May 2015: http://www.hcss.nl/reports/download/164/2938/
[25] Gehem et al. 2015, p. 9
[26] Gehem et al. 2015, p. 9
[27] ENISA. 2013. *National-level Risk Assessments: An Analysis Report*. As of 12 October 2015: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report/at_download/fullReport

geographical spread, since the study team wanted to include threat assessments from inside as well as outside the EU.

Even though these threat assessments may be considered authoritative, on the basis that the authoring organisations are key players and experts in the field, caveats about their findings must be emphasised, due to the quality of underlying sources and their methodological approach. These threat assessments rely on external sources, including private sector and media reports. Although private sector reports contain valuable threat intelligence, considering their for-profit nature, it is difficult to classify their analysis as objective. A similar caveat must be mentioned for media reports,[28] which may be inaccurate or incomplete (see Section 2.10).

Another limitation of the use of these existing threat assessments is that, to varying degrees, they rely on each other (see Section 2.3). Further, each threat assessment has a different purpose and therefore a different focus; this means certain threats, actors, and tools may be overemphasised. As such, stating that *n* number of reports mentions a particular type of threat and subsequently using this as an indicator for the *urgency* or *severity* of the threat may be misleading. As a result, the following sections count the number of times a specific threat, actor or tool is mentioned only as a proxy measure to indicate their presence – not importance – in the cyberthreat landscape.

The overview of threat components is substantiated by drawing on qualitative findings of the threat assessments and supplemented whenever possible with examples of incidents occurring this year (2015). These examples have been located via Google News and serve merely as illustrations; they are not intended to be representative or generalisable but aim to help the reader understand how such a threat may evolve into practice. As a final note, it is crucial to mention that this overview is not comprehensive. It highlights selected threat actors and tools, the rationales behind which will be discussed in the following sections. The threat assessments included in our analysis are shown in Table 2.

Table 2. Threat assessments

Report Name	Geographic Coverage	Publication Year
ACSC – Threat Report	Australia	2015
BSI – State of IT Security in Germany	Germany (Also incidents in the UK and Austria)	Nov. 2014
ENISA – Threat Landscape (ETL)	No geographic delineation indicated	Dec. 2014
Europol – Internet Organised Crime Threat Assessment (iOCTA)	European Union	2014
NCSC – Cyber Security Threat Assessment the Netherlands (CSAN)	The Netherlands (Also includes important developments abroad)	Oct. 2014
Verizon – Data Breach Investigations Report (DBIR)	Global coverage (61 countries)	2015

Source: RAND Europe study team

[28] ENISA's Threat Landscape, for example, quotes the *Daily Mail* as a source in its report. ENISA. 2015a. *ENISA Threat Landscape 2014*. As of 14 September 2015: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

2.5 Threat targets identified

To understand why a threat is perceived as such, it requires a connection to a target with specific interests that a perpetrator wants to influence. This section identifies these targets and interests. In cybersecurity threat assessments, targets generally include individuals (consumers and citizens), governments and corporations. Threats can implicate more than one target but the consequences may be different for each target because they hold different interests. CSAN identifies four main categories of interest: individual, organisational, supply chain and societal (see Figure 1).

Figure 1. Targets and their interests[29]

Source: RAND Europe study team

The financial interest of individuals is missing from the identification of subinterests in Figure 1, but overall the breakdown provided by NCSC illustrates the targets as well as what is being *threatened*. The identification of targets' interests helps to develop an understanding of why a particular threat actor may want to carry out a cyberattack. In this sense targets' interests connect with threat actors' motives, as we discuss in the next section.

2.6 Threat actors categorised

Threat actors – often also referred to as threat agents – are the individuals or groups that carry out or intend to carry out cyberattacks. The potential for them to do so leads to the establishment of a threat. This section follows an actor-centric approach, identifies three categories of threat actors (states, profit-driven criminals and hacktivists and extremists) and highlights the findings from the threat assessments connected to each.

[29] National Cyber Security Centre (NCSC). 2014. *Cyber Security Assessment Netherlands - CSBN 4*. As of 15 June 2015: https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/cyber-securty-assessment-netherlands-4-cybercrime-and-digital-espionage-remain-the-biggest-threat/1/CSAN%2B4.pdf, p.18

The disadvantages of an actor-centric approach arise primarily from the challenges of classifying actors in the cyber domain and attributing threats to them. Klimburg & Tirmaa-Klaar state: 'The differences between cybercrime, cyberterrorism and cyberwarfare are often difficult to ascertain, and often lie in the eye of the beholder.'[30] As the authors attest, this is not purely due to technical reasons, even though attribution remains an ongoing challenge in the cyber realm. Instead, according to them, there is 'a principle problem with the separation of cyberattacks into such actor-based categories as "criminal", "terrorist" and "soldier"' because 'these identities themselves can be fluid and ambiguous. Even if the attacking individual can be identified, it is perfectly possible for a cybercriminal to engage in cyberwarfare acts disguised as a cyberterrorist.'[31] Using threat actors as the basis for classification therefore faces two difficulties. The first is technical, in the sense that attribution is difficult because threat actors can hide or alter the origins of the attack. The second is the subjective nature of classification. These two issues must be borne in mind when discussing threat actors, especially when a threat is connected to a particular actor on the basis of past events.

Nevertheless, there are benefits to the actor-centric approach. Contrary to an incident-centric approach, which typically starts with the discovery of an event and potentially ends with attribution, the actor-centric approach seeks to understand the motivations of specific, known threat actors. By ascribing certain tactics, technologies and procedures (TTPs), and ultimately an incident of compromise (IOC), to the threat actors, the actor-centric approach reverses the reactive order of an incident-centric approach.[32] The rich context generated around the actors targeted enables organisations to be proactive, even, predictive. Triangulation of information seems to be key:

> *With regards to the actor-centric approach, one could argue whether it is actionable or not. On its own and in isolation it probably isn't, but when fused, stored and correlated with your own organization's data/information and other sources of information it can be both predictive and actionable.*[33]

The inclusion of a discussion on threat actors is therefore merely a piece of the overall puzzle, but a viable one to understand who may potentially want to threaten a particular interest, as listed in Section 2.5.

For the purposes of this study, the scope of threats posed by actors is limited to deliberate attacks, even though we acknowledge the existence of other threats, such as unintentional disruption and outages caused by human error, environmental causes or technology failure. The identification of threat actors is also limited to three main categories. This categorisation is loosely based on Clapper.[34] He identifies:

- Nation states with highly sophisticated cyber programmes, such as Russia and China.

[30] Klimburg, Alexander & Heli Tirmaa-Klaar. 2011. *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*. Study for the European Parliament's Subcommittee on Security and Defence. As of 12 October 2015: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf, p. 5
[31] Klimburg & Tirmaa-Klaar 2011, p. 5.
[32] Arena, Mark. 2015. 'Cyber threat intelligence: Comparing the incident-centric and actor-centric approaches.' *Intel471*. As of 12 October 2015: http://www.intel471.com/blog-incident-centric-versus-actor-centric.html
[33] Arena 2015.
[34] Clapper, James R. 2015. *Worldwide Threat Assessment of the US Intelligence Community – Statement for the Record*. Senate Armed Services Committee, February 26. As of 12 October 2015: http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-26-15.pdf

- Nation states with less sophisticated cyber programmes but potentially more disruptive intent, such as Iran and North Korea.
- Profit-driven criminals.
- Ideologically motivated hackers or extremists.[35]

Perhaps the most essential aspect of Clapper's classification is that he identifies ideologically motivated hackers or extremists, rather than a category for cyberterrorists. The concept and notion of cyberterrorism is controversial, as it is possibly the most politicised type of categorisation available. As Heickerö puts it, 'For an attack to be regarded as cyberterrorism, the intended effect has to be serious human and economic casualties, intense fear and anxiety – terror – among the citizens. Whether or not a cyberattack against vital information infrastructure is viewed as an act of terrorism depends on the intent.'[36] The concept of casualties as a condition or feature does not translate neatly into cyberspace, particularly for a number of incidents that some have labelled as cyberterrorism.

In order to map the threat actors, the study team searched for key words in each of the six threat assessments to identify which actors were mentioned and how often (see Table 3). This means that rather than restricting our search to a precise threat category, for instance 'states', we have also searched for words with similar meanings or implications, such as 'nation states', 'state-sponsored', and 'state actor' (see footnotes). Likewise, the study team recognised differently spelled and punctuated terms, such as 'cybercriminals', 'cyber-criminals', and 'cyber criminals'. The numbers indicated in brackets therefore represent the sum of such mentions in each threat assessment.

Table 3. Threat actors

Report[37]	**Threat actors**		
	States	Profit-driven cybercriminals	Hacktivists and extremists
ACSC	Yes (13)[38]	Yes (4)[39]	Yes (4)[40]
BSI	No (0)[41]	Yes (11)[42]	Yes (9)[43]
ENISA	Yes (21)[44]	Yes (34)[45]	Yes (27)[46]
Europol	No (3)[47]	Yes (81)[48]	No (4)[49]

[35] Clapper 2015.
[36] Heickero, Roland. 2014. 'Cyber Terrorism: Electronic Jihad.' *Strategic Analysis* 38(4): 554-565
[37] For full titles of the threat assessment reports, see Table 2.
[38] 'nation state' (3); 'nation-state' (0); 'state-sponsored' (10); 'state sponsored' (0); 'state actor' (0)
[39] 'cybercriminal' (2); 'cyber criminal' (2); 'cyber-criminal' (0)
[40] 'hacktivist' (3); 'terrorist' (1); 'extremist' (0)
[41] 'nation state' (0); 'nation-state' (0); 'state-sponsored' (0); 'state sponsored' (0); 'state actor' (0)
[42] 'cybercriminal (11); 'cyber-criminal' (0); 'cyber criminal' (0)
[43] 'hacktivist(s)' (8); 'terrorist' (0); 'hackers' (1); 'extremist' (0)
[44] 'nation state' (13); 'nation-state' (0); 'state-sponsored' (4); 'state sponsored' (4); 'state actor' (0)
[45] 'cybercriminal' (9); 'cyber criminal' (5); 'cyber-criminal' (20)
[46] 'hacktivist' (16); 'terrorist' (11); 'extremist' (0)
[47] 'nation state' (2), however not in relation to cyberthreats; 'nation-state' (0); 'state-sponsored' (1), however not in relation to cyberthreats; 'state sponsored' (0); 'state actor' (0)
[48] 'cybercriminal' (71); 'cyber criminal' (10); 'cyber-criminal' (0)
[49] 'hacktivist' (0); 'terrorist' (2), however not in relation to cyberthreats; 'extremist' (2), however not in relation to cyberthreats

NCSC	Yes (57)[50]	Yes (34)[51]	Yes (37)[52]
Verizon	Yes (3)[53]	Yes (1)[54]	Yes (9)[55]

Source: RAND Europe study team

2.6.1 States

Of the six threat assessments, states were mentioned as a threat actor in four (see Table 3). Nation states have evolved into a threat actor and can potentially threaten a variety of targets, ranging from other states to citizens. Nation states may aim to target other states for geopolitical reasons. They may also target citizens through, for example, surveillance to gain access to information held by citizens or private communication exchanged between them. From the perspective of the NCSC of the Netherlands, the greatest threat to the government and the business community stems from state actors – as well as profit-driven cybercriminals (see Section 2.6.2).[56] More specifically, the threat of digital espionage exercised through state actors has increased, in terms of number of cases, complexity and impact.[57]

Furthermore, the NCSC states that nearly every intelligence agency has invested in the development of digital capabilities, which means digital espionage is no longer an ability reserved for the few. This is a noteworthy observation in light of Clapper's distinction between more and less sophisticated states. From the perspective of the NCSC this distinction may no longer be that straightforward, which could potentially alter the threat landscape. The Australian Cyber Security Centre (ACSC) echoes the observation made by the NCSC in indicating that the number of states with capabilities will continue to increase.[58] Cases of digital espionage have featured prominently in the media. Notable examples include the revelations made by Edward Snowden about the US National Security Agency (NSA), as well as practices of the Hacking Team, which came to light after the company had been breached and its data had been made public by the perpetrators.

In its assessment, the NCSC notes:

> *The intelligence services have no evidence that in the past few years allies have deployed digital espionage activities against the Netherlands. However, the threat from non-allies is considered to be present and increasing*.[59]

2.6.2 Profit-driven cybercriminals

Cybercriminals are mentioned in each of the six threat assessments (see Table 3). The primary motivation of profit-driven cybercriminals is financial gain. Therefore the primary target of these criminals is often the financial services and retail sectors.

[50] 'nation state' (0); 'nation-state' (0); 'state-sponsored' (3); 'state sponsored' (0); 'state actor' (54)
[51] 'cybercriminal' (0); 'cyber criminal' (33); 'cyber-criminal' (1)
[52] 'hacktivist' (23); 'terrorist' (14); 'extremist' (0)
[53] 'nation state' (0); 'nation-state' (0); 'state-sponsored' (3); 'state sponsored' (0); 'state actor' (0)
[54] 'cybercriminal (1); 'cyber criminal' (0); 'cyber-criminal' (0)
[55] 'hacktivists' (0); 'hacktivist' (0); 'hackers' (9); 'extremists' (0); 'extremist' (0)
[56] NCSC 2014.
[57] NCSC 2014, p. 8.
[58] Australian Cyber Security Centre (ACSC). 2015. *2015 Threat Report*. Canberra: Australian Government. As of 12 October 2015: https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf
[59] NCSC 2014.

Cybercrime has become a service, where specialisation and the existence of underground markets have allowed a flourishing business in which even criminals without any technical skills can engage in cybercrime activities.[60] This has been acknowledged by various sources including Europol[61] and the ACSC.[62] The NCSC also refers to the professionalisation of criminal services. Botnets can be rented; credit card information and other relevant personal data can be purchased along with other 'goods' that can subsequently be abused for financial gain.

An example of a recent incident involving profit-driven criminals was the takedown of the Darkode forum.[63] Before the takedown, Darkode had been in operation since 2007 as an online marketplace that catered for profit-driven criminals who used it to buy and sell hacking tools, zero-day exploits, ransomware, stolen credit card numbers and other banking data, as well as spamming and botnet services. The aim of taking down marketplaces like Darkode is to cut off the supply of cybercrime tools. According to Hickton, 'Of the roughly 800 criminal Internet forums worldwide, Darkode represented one of the gravest threats to the integrity of data on computers in the United States and around the world and was the most sophisticated English-speaking forum for criminal computer hackers in the world.'[64]

Europol also describes how the evolution of the professionalisation and industrialisation of cybercrime has allowed more traditional organised crime groups to enter the cybercrime arena: 'Traditional organised crime groups (OCGs), including those with a mafia-style structure, are beginning to use the service-based nature of the cybercrime market to carry out more sophisticated crimes, buying access to the technical skills they require. This trend towards adopting the cybercrime features of a more transient, transactional and less structured organisational model may reflect how all serious crime will be organised in the future.'[65]

According to the NCSC, profit-driven cybercriminals – along with states – pose the greatest threat to governments and the business community. This is particularly evident with respect to incidents of unauthorised access (see Section 2.8.1) where perpetrators make use of banking trojans (see Section 2.7.1.1), ransomware (see Section 2.7.1.2) or point of sale (PoS) malware (see Section 2.7.1.1). This list is not exhaustive but it includes the main threat tools used by profit-driven cybercriminals. The main targets of this threat actor include the financial services industry, namely financial service providers, organisations within the retail sector and consumers.

2.6.3 Hacktivists and extremists

Hacktivists and extremists are mentioned in five of the threat assessments (see Table 3). This category distinguishes itself from other threat actors in terms of its motive and desire for visibility. Hacktivists use digital means to express their ideological or political intentions or motivations. The NCSC defines hacktivists as 'people who use their cyberattacks to realise ideological aims or to bring such aims closer. The aims vary

[60] Barwick, Hamish. 2015. 'Cybercrime-as-a-service on the rise says government report.' *ComputerWorld*, July 29. As of 12 October 2015: http://www.computerworld.com.au/article/580687/cybercrime-as-a-service-rise-says-government-report/
[61] Europol. 2014a. *The Internet Organised Crime Threat Assessment (iOCTA)*. As of 12 October 2015: https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf
[62] Barwick 2015.
[63] Zetter, Kim. 2015. 'Dozens nabbed in takedown of cybercrime forum Darkode.' *Wired*, July 15. As of 12 October 2015: http://www.wired.com/2015/07/dozens-nabbed-takedown-cybercrime-forum-darkode/
[64] US DoJ. 2015a. 'Major computer hacking forum dismantled.' *Justice News*, July 15. As of 12 October 2015: http://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled
[65] Europol 2014a.

amongst and within groups of hacktivists and over time.'[66] With respect to developments demonstrated by this threat category, the NCSC observes that there are no reliable figures to assess whether the number of hacktivistic cyberattacks changed in 2013.[67] Hacktivists rely on three main methods to accomplish their goals: DDoS attacks (see Section 2.8.5); disclosure (see Section 2.8.3); and defacement (see Section 2.8.4).

2.7 Threat tools explained

This section focuses on tools and highlights a number that are frequently discussed in the six threat assessments. In making a selection of threat tools, the study team focused on technological tools, excluding more complex methods such as insider threats and social engineering. The threat tools explained in this section are malware, Trojans, ransomware, PoS malware, botnets and exploits. Another variant of malware, the remote access tool (RAT), will be discussed separately in relation to a case study in Chapter 5 (see Section 5.3.2).

Table 4 shows whether these threat tools have been mentioned in the six threat assessments, and if so, how many times. Breaking down threat tools in a taxonomically justified manner is challenging, especially since malware – as will become evident – permeates almost all threat tools. Yet, some forms of malware deserve specific identification because of their impact or characteristics.

The method used for the search is identical to that of mapping the threat actors (see Section 2.6) and the details of the search can be found in the footnotes.

Table 4. Threat tools

Report[68]	Threat tools					
	Malware[69]	(Banking) Trojans[70]	Ransom-ware[71]	PoS[72]	Botnets[73]	Exploits[74]
ACSC	Yes (39)	Yes (3)	Yes (19)	No (0)	Yes (9)	Yes (23)
BSI	Yes (113)	Yes (4)	Yes (10)	Yes (1)	Yes (22)	Yes (30)
ENISA	Yes (87)	Yes (40)	Yes (25)	No (0)	Yes (59)	Yes (98)
Europol	Yes (115)	Yes (8)	Yes (23)	Yes (1)	Yes (39)	Yes (8)
NCSC	Yes (113)	Yes (4)	Yes (89)	Yes (3)	Yes (39)	Yes (92)
Verizon	Yes (107)	Yes (1)	Yes (2)	Yes (32)	Yes (6)	Yes (9)

Source: RAND Europe study team

[66] NCSC 2014.
[67] NCSC 2014.
[68] For full titles of the threat assessment reports, see Table 2.
[69] 'malware'
[70] 'trojan'
[71] 'ransomware'
[72] 'point-of-sale'
[73] 'botnet'
[74] 'exploit'; 'exploit kit'

2.7.1 Malware

As Table 4 demonstrates, malware has an overwhelming presence in the cybersecurity threat landscape. In its DBIR, Verizon describes how 'Malware is part of the event chain in virtually every security incident'.[75] 'Malware' is shorthand for malicious software and therefore applies to a wide range of 'products' that enable perpetrators from various backgrounds, ranging from states to profit-driven cybercriminals, to gain unauthorised access. According to the NCSC, the amount of malware continues to increase greatly every year. The German Ministry of the Interior has stated there are at least 1 million malware infections a month in Germany.[76] Europol also indicates that 'the changes in the production of malware are increasing rapidly in scale and sophistication'.[77]

Often 'new' malware represents variations of existing malware. Alterations to an existing form can allow perpetrators to circumvent detection systems. These variations have only a short lifespan, as indicated by the NCSC. Due to the continuous introduction of variations, as well as the short life of malware, there is a pressing question about the effectiveness of 'traditional' anti-virus protection, which is based on 'signature' recognition. This requires awareness of the existence of a particular type of malware so that the system can detect it. If the anti-virus product does not contain the signature, it cannot detect the virus effectively. This raises the question of whether other forms of protection need to be introduced.[78] This question is not new and is a challenge that has previously been identified. [79] Europol also describes how 'malware is becoming increasingly "intelligent". Some malware includes code to prevent it either being deployed or run in a sandbox environment, as used by malware researchers for analysis. In this way malware developers can avoid automated analysis of their product, thereby remaining undetected for longer. Malware developers will continue to refine their products to make them stealthier and harder to detect and analyse.'[80]

Europol even refers to Malware-as-a-Service (MaaS) and notes that 'MaaS is becoming increasingly professional, mirroring legitimate commercial software development companies by providing functionality such as 24/7 customer support and frequent patches and updates to continually refine their product and increase its capability and competitiveness in the malware marketplace.'[81]

2.7.1.1 (Banking) Trojans

Trojans are also mentioned in each of the six threat assessments, albeit to a lesser degree (see Table 4). Europol describes banking malware, often referred to as banking Trojans, as the 'work horse' of the digital underground. Banking Trojans harvest log-in credentials of victims that allow unauthorised access to their accounts (see Section 2.8.1). According to the German Ministry of the Interior, Trojans are one of the most frequently detected types of malware. [82] Interviewees specifically identified banking Trojans as the most urgent threat and Europol indicates that over half of EU Member States reported cases that related to banking Trojans. Among the most notorious

[75] Verizon 2015, p. 49.
[76] BSI 2014, p. 16.
[77] Europol 2014a.
[78] NCSC 2014.
[79] See: van der Meulen, Nicole S. 2011. 'Between Awareness and Ability: Consumers and financial identity theft.' *Communications & Strategies* 81
[80] Europol 2014a, p. 27.
[81] Europol 2014a, p. 23.
[82] BSI. 2014, p. 16.

malware is Zeus, which is 'unparalleled in scope, use and effectiveness'.[83] Zeus was first discovered in 2007 in a credential-theft against the United States Department of Transportation, and has since stolen hundreds of millions of dollars by attacking, among others, prominent corporations, banks and government agencies. In 2011, its creator released the source code, resulting in its unprecedented spread.[84] Today, nearly every banking Trojan embeds some component of Zeus.[85]

Besides Zeus, Europol also identifies Citadel as another common variant of banking Trojans. Citadel is Zeus-incorporated compound malware, adopting an open-source development model, which allows anyone to improve (worsen) the product. [86] Contributions include Advanced Encryption Standard (AES) encryption, command and control, evasion tactics against tracking sites and remote recording of victims' activities. Taking advantage of its adaptability and growth, Citadel made huge gains for its operators, until a takedown initiative by a Microsoft-led coalition disabled nearly 88 per cent of its infections.[87]

2.7.1.2 Ransomware

Like malware and Trojans, ransomware appears in all six threat assessments and is recognised as a prominent threat tool (see Table 4). Ransomware distinguishes itself from other malware through its functionality and, arguably, its visibility. Operators of ransomware seek financial gain by infecting computer systems and making them deny their users access unless a ransom has been paid. Europol describes how ransomware was first discovered in 1989 but resurged in 2013. According to Europol's calculations, approximately 65 per cent of law enforcement agencies in the EU have encountered some form of ransomware, predominantly 'police ransomware'.

CryptoLocker and CryptoWall are two examples of ransomware products. Both work by encrypting files and documents that they infect and deleting the original copies. The victims are then notified about the infection and asked to pay a sum to have their files back. According to researchers, nearly 30 per cent of CryptoLocker and CryptoWall victims pay the ransom, making these products profitable enterprises.[88]

Besides its high success rate, ransomware affects users of computer systems globally despite its heavy reliance on social engineering techniques and knowledge of language skills. [89] Enhancing the information provided by the threat assessments, Symantec's telemetry ranks countries like the US, Japan, the UK, Italy, Germany and India as the countries most impacted by ransomware, demonstrating the geographic spread of its operation.[90] Symantec also warns that current-generation ransomware can easily 'make the leap from mobile phones to wearable devices such as smartwatches'.[91] In 2013,

[83] Donohue, Brian. 2013. 'The big four banking Trojans.' *Kaspersky Lab Daily*, October 21. As of 12 October 2015: https://blog.kaspersky.com/the-big-four-banking-trojans/
[84] Tamir, Dana. 2014. 'ZeuS.Maple variant targets Canadian online banking customers.' *Security Intelligence*, June 9. As of 12 October 2015: https://securityintelligence.com/zeus-maple-variant-targets-canadian-online-banking-customers/#.VczBw01RHcs
[85] Donohue 2013.
[86] Tamir 2014.
[87] Donohue 2013.
[88] Pinson, Richard. 2015. 'Computer threat: Cryptolocker virus is ransomware.' *Nashville Business Journal*, August 10. As of 12 October 2015: http://www.bizjournals.com/nashville/blog/2015/08/computer-threat-cryptolocker-virus-is-ransomware.html
[89] NCSC 2014, p. 83.
[90] FP Staff. 2015. 'The dawn of ransomwear: How ransomware could move to wearable devices.' *First Post*, August 10. As of 12 October 2015: http://www.firstpost.com/business/dawn-ransomwear-ransomware-move-wearable-devices-2385712.html
[91] FP Staff 2015.

Microsoft indicated that ransomware was on the rise, especially in Europe.[92] And in 2014 the NCSC noted that ransomware was getting more innovative and aggressive.[93] The prospects of ransomware's evolution remain worrisome and various organisations have issued alerts against this malware, including the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3).[94]

2.7.1.3 Point of sale (PoS) malware

Although it is mentioned in just four threat assessments, this particular type of malware deserves further explanation due to its potentially debilitating impact (see Table 4). PoS malware copies credit card data from consumers through check-out systems used in retail. One of the most well-known examples was an attack on Target – a major US retailer. Osborne states:

> *The [PoS] malware can scan, capture and send both track one and track two payment card data to a waiting command-and-control (C&C) center. Track one contains a cardholder's name and account number, while track two, most commonly used, stores information relating to the card holder's account, encrypted PIN and other data.*[95]

2.7.1.4 Botnets

Botnets appear as a threat tool in all six threat assessments (see Table 4). A bot is remotely controllable malware that is covertly installed and allows for the unauthorised use of an infected system. A botnet is a collection of infected systems controlled centrally via command-and-control servers. Botnets are the backbone of the cybercriminal infrastructure as they provide criminals with 'immense resources of computer capacity and bandwidth'[96] to conduct grand-scale information theft and banking fraud, launch DDoS attacks and send out high volumes of spam,[97] phising emails, e-mails with malware attachments and mining cryptocurrencies (e.g. BitCoins), and disseminate ransomware – to name just a few activities.[98]

While ENISA and the NCSC recognise that the number of botnets has dropped in absolute terms, due to multiple successful law enforcement takedowns, they also emphasise that botnet efficiency has increased significantly.[99] Botnet operators are going to great lengths to disguise and defend their botnets, through the use of peer-to-peer (P2P) networks, domain generating algorithms (DGA) and the deployment of polymorphic malware.[100]

Recognising this, Europol highlights that 'with today's methods a large botnet is not always required to launch a large-scale attack'. [101] The ASCS echoes this assessment by

---

[92] Gerden, Eugene. 2015. 'FINcert to help Russian banks respond to cyber attacks.' *SC Magazine UK*, July 10. As of 12 October 2015: http://www.scmagazineuk.com/fincert-to-help-russian-banks-respond-to-cyber-attacks/article/425701/
[93] NCSC 2014.
[94] Pinson 2015.
[95] Osborne, Charlie. 2015. 'Retailers targeted by new point-of-sale malware through job requests.' *ZDnet*, May 26. As of 12 October 2015: http://www.zdnet.com/article/internships-become-bait-to-infect-retailers-with-new-point-of-sale-malware/
[96] BSI 2014, p. 18.
[97] Europol 2014a, p. 46.
[98] BSI 2014, p. 18; Europol 2014a, p. 25; NCSC 2014, p. 32; ENISA 2015a, p. 19; Verizon 2015, p. 22; ACSC 2015, p. 17.
[99] ENISA 2015a, p. 19; NCSC 2014, p. 32.
[100] NCSC 2014, p. 32; Europol 2014a, p. 10, 25; Verizon 2015, p. 22; For additional information see the Beebone case study in this report.
[101] Europol 2014a, p. 21.

noting that 'even relatively small botnets can cause significant problems for Australian organisations'. [102] However, the trend towards smaller and more resilient botnets contrasts starkly with the emerging trend of web server based botnets and hardware based/mobile botnets through the spread of the Internet of Things and cloud services.[103] As a result the 'the prices for deploying botnets […] are dropping, because of the numerous other options that are available'.[104]

Botnets are also an integral part of the 'industrialisation of cybercrime' as their services are freely available on the black market. This in turn contributes to the lowering of the overall entry threshold and the costs associated with conducting cyberattacks.[105]

2.7.1.5 Exploits

Exploits are mentioned as threat tools in all six threat assessments (see Table 4). According to the NCSC, exploits are defined as 'software, data or a series of commands that exploit a hardware and/or software vulnerability for the purpose of creating undesired functions and/or behaviour'.[106] Exploits are not malicious per se; security researchers also use them to demonstrate the existence of software and hardware vulnerabilities.[107] However, exploits do form the basis for every malware product currently in existence.[108]

The most prominent tool is the exploit kit. Exploit kits are fully automated toolkits that systematically search for unpatched vulnerabilities on user end-devices for the purpose of downloading malicious content.[109] As such, exploit kits contribute significantly to lower entry-level thresholds for cybercrime and 'represent one of the most common methods of infections with more than 80 per cent of online threats detected in 2012'.[110]

The most popular methods of deploying exploit kits are targeted (Watering Hole) and not-targeted (drive-by) attacks.[111] In a Watering Hole attack, exploit kits are deployed to infect particular websites, targeting participants in specific conferences, political topics or social causes. For example, Watering Hole attacks were responsible for the breaches of Facebook, Twitter, Apple and Microsoft in 2013.[112] Drive-by attacks are usually not targeted and rely on malvertisements[113] or other compromised website elements to scan, redirect and then infect visitors.[114] In both instances the exploit kit scans and exploits unpatched vulnerabilities and in very rare cases applies a zero-day exploit, meaning an exploit of an unknown vulnerability for which no patch or fix yet exists.[115]

Exploit kits have become very complex and sophisticated tools that trend towards infecting targets with file-less malware or using TOR communications.[116] Defeating exploit kits is particularly difficult, as was illustrated by the arrest in 2013 of 'Paunch',

[102] ACSC 2015, p. 17.
[103] ENISA 2015a, p. 19; Europol 2014a, p. 21, 25; BSI 2014, p. 18.
[104] NCSC 2014, p. 23-24; Europol 2014a, p. 25; BSI 2014, p. 18.
[105] NCSC 2014, p. 32; BSI 2014, p. 18.
[106] NCSC 2014, p. 105.
[107] ACSC 2015, p. 22.
[108] NCSC 2014, p. 29.
[109] ENISA 2015a, p. 25.
[110] Europol 2014a, p. 23.
[111] ACSC 2015, p. 13; BSI 2014, p. 18; NCSC 2014, p. 57.
[112] Europol 2014a, p. 23.
[113] BSI 2014, p. 18.
[114] BSI 2014, p. 17.
[115] BSI 2014, p. 18.
[116] ENISA 2015a, p. 25.

the developer of the Blackhole Exploit Kit (BEK). While BEK had almost disappeared by 2014, new exploit kits quickly filled the gap and cybercriminals learned to adapt.[117]

2.8 Threats types described

This section describes and discusses the threat types identified in the six existing threat assessments. Threats are categorised according to the five types of threat identified in the NIST definition (see Section 2.2). These threat types can be connected to the core principles of the concept of information security: confidentiality, integrity and availability.[118] These can be mapped as shown in Figure 2.

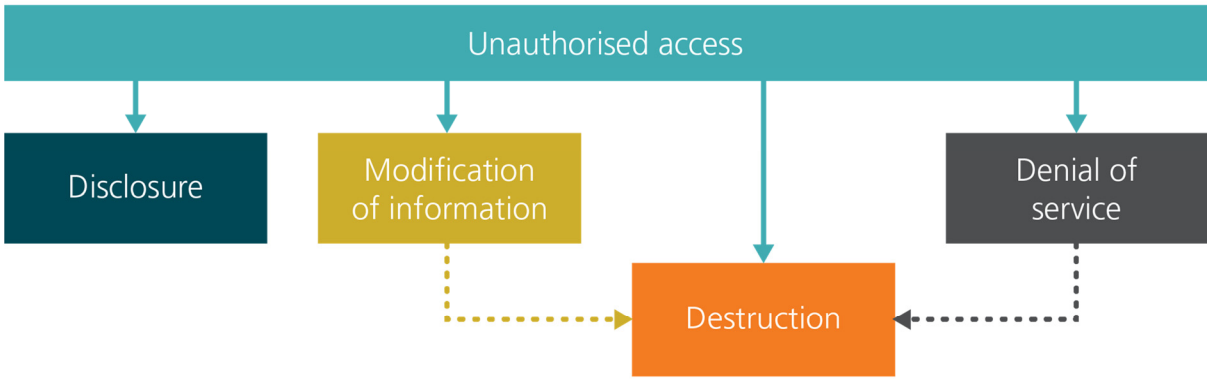
Figure 2. Threat types and information security principles

Source: RAND Europe study team

Using the definition of threats and types of threat described in Figure 2, a clear link can be established between information security (cybersecurity), threat definition and subsequent threat types. However, this does not mean the threat types are mutually exclusive or independent. For example, unauthorised access can be used as an overarching threat type that may lead to any of the other four threat types. A perpetrator who has unauthorised access to information or an information system can destroy either or both and disclose or modify the information itself. Denial of service could theoretically be accomplished without gaining unauthorised access, although the use of botnets means the perpetrator first needs unauthorised access to other computers before being able to leverage them for a DDoS attack (see Section 2.8.5). The connection between the threat types is illustrated in Figure 3.

[117] ENISA 2015a, p. 25.
[118] National Institute of Standards and Technology (NIST). 2004. Standards for Security Categorization of Federal Information and Information Systems. FIPS PUB 199. As of 12 October 2015: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Figure 3. Threat types and their connections



Source: RAND Europe study team

The main aim is to develop a more robust and clear framework for future threat assessments and analyses. As Verizon puts it, 'While the threats against us may *seem* innumerable, infinitely varied, and ever changing, the reality is they aren't'.[119] At this stage, however, it bears repeating that threats are not mutually exclusive, since there are interdependencies (see Section 2.2). For example, data breaches lead to potential disclosure of sensitive personal or financial data, which may then be used to gain unauthorised access to bank accounts. The following sections will delve deeper into each threat type.

2.8.1 Unauthorised access

Unauthorised access is a meta-threat since once inside perpetrators can carry out a number of other activities such as disclosure, modification of information, destruction as well as DDoS. In this sense, preventing unauthorised access is the primary means to prevent other types of threats.

Unauthorised access therefore is often connected to different threat actors, but especially profit-driven cybercriminals and states. From a profit-driven cybercriminal perspective, unauthorised access may pave the way to commit various forms of fraud, since such unauthorised access allows them to misuse the identity of another individual (identity fraud) or drain an existing bank account (account takeover). Europol's Internet Organised Crime Threat Assessment (iOCTA) describes how e-commerce related fraud has increased, in line with the growing number of online payments.[120] This affects major industries such as airlines and hotels in particular. A factor associated with the increase in e-commerce related fraud are large-scale data breaches that lead to the compromise of financially sensitive data such as credit and debit card numbers. These are subsequently sold on underground forums, which can be monetised through e-commerce related fraud.[121]

Data breaches form a focal point of threat discussions (see Section 2.1). However, data breaches are an overarching category that deserves greater attention, especially with respect to the financial services and retail sectors. Unauthorised access can occur through PoS intrusions (see Section 2.7.1.1), as Verizon has testified.[122] The company

[119] Verizon 2015.
[120] Europol 2014a, p. 12.
[121] Europol 2014a, p. 12.
[122] Verizon 2015, p. 31.

states that even though this type of intrusion is not new, the methods used to attack payment systems have become more varied. PoS intrusions affect both small and larger organisations, predominantly in the accommodation, retail and entertainment sector. PoS intrusions provide perpetrators with access to financially sensitive data that can – as indicated in Europol's report – facilitate e-commerce fraud in general and identity fraud in particular.

Closely related to PoS intrusions are payment card skimmers. These devices allow perpetrators access to the financially sensitive data held on the magnetic strip on the back of a bank or credit card. This type of threat mainly affects the financial services industry and retail sectors.

To gain unauthorised access, perpetrators still deploy social engineering techniques like phishing to trick people into breaking security procedures. The purposes of this unauthorised access range from crime to espionage. Verizon has been able to provide more in-depth insight: 'The vector of malware installation is mostly through phishing, but was split between either attachments or links, and malware installed through web drive-by has made a stronger-than-normal appearance this year.'[123] Van der Meulen describes this transformation as a shift from 'voluntary' to 'involuntary' facilitation.[124]

Apart from attempts to gain unauthorised access, existing threat assessments also focus on digital or cyberespionage. The NCSC describes the loss of control over information as a real threat, in particular with respect to intelligence services (see Section 2.6.1), a concern echoed by BSI.[125]

2.8.2 Destruction

The threat of destruction can affect both information and information systems. Certain threat assessments contain closely related categories. In CSAN-4, the NCSC refers to digital sabotage, which is perhaps best classified as either the destruction or modification of information, depending on modus operandi. Modification of information and destruction can also occur in tandem, if perpetrators first modify information with the intent to destroy (see Section 2.2). Again, this illustrates the interdependency of threats. In its category of digital sabotage, the NCSC notes: 'A number of examples of a new form of digital sabotage occurred worldwide in 2013, whereby state actors were possibly involved. These involved the deliberate removal or destruction of large quantities of data from commercial networks in countries that were considered by the attackers to be their political opponents. Examples include the attacks on the government of Qatar and a large-scale attack on South Korean commercial networks resulting in disruptions in the financial sector.'[126]

Destruction of data can lead to fatal consequences. The German Ministry of the Interior describes the case of a collaboration and development platform for software developers operated by the company Code Space.[127] The platform became the target of a DDoS attack in June 2014 that lasted for 48 hours. The company refused to pay the extortion fee demanded and the perpetrators deleted nearly all their data, back-ups and machine settings. This destruction of information led to the discontinuation of the company's operation because of the cost of financial restoration and compensation to clients.

[123] Verizon 2015, p. 53.
[124] Van der Meulen 2011.
[125] BSI 2014, p. 14.
[126] NCSC 2014, p. 71.
[127] BSI 2014, p. 14.

Destruction can also occur if perpetrators use ransomware (see Section 2.7.1.2), which works on the basis of extortion, i.e. the threat of destruction of data if the individual or organisation targeted refuses to pay the ransom. Destruction of data may occur if payment is refused.

2.8.3 Disclosure

Unauthorised access to information and information systems can be acquired for the purposes of abuse. Examples include e-commerce and other forms of fraud. The alternative 'consequence' of unauthorised access is public disclosure of the data. A recent and well-publicised disclosure that affected consumers in both the US and the EU was the Ashley Madison hack. Ashley Madison is a website that facilitates meetings between users who want to engage in extramarital affairs. It allegedly has 37 million users,[128] although another source quotes a global user database of 29 million.[129] Other sources claim many of the profiles are fake. The hacktivist group responsible for the breach – self-identified as The Impact Team – published users' personal information. This breach and subsequent disclosure came, as Krebs notes, less than two months after intruders hacked and compromised personal information from users of AdultFriendFinder.[130] The Impact Team infiltrated the Ashley Madison database to prove that Avid Life Media (ALM), the company that owns the website, did not actually delete user profiles despite receiving requests from users and a $20 payment per deleted profile.[131] The Impact Team proved its argument by publishing user profiles that should have been deleted and therefore unavailable. The Impact Team specifically stated: 'Avid Life Media has been instructed to take Ashley Madison and Established Men offline permanently in all forms, or we will release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails. The other websites may stay online.' [132] Public disclosure is a type of threat exercised by predominantly hacktivists (see Section 2.6.3), but more generally disclosure is also a threat type affiliated with profit-driven criminals (see Section 2.6.2), especially as they sell personal information or other relevant data on underground forums.

2.8.4 Modification of information

Our review of existing threat assessments threats suggests that modification of information appears to play a less prominent role, perhaps because this is a less frequently used threat category and may be embedded in other categories, such as digital disruption, digital sabotage or unauthorised access. In the ETL, modification is briefly mentioned in connection with threats to mobile phone applications where perpetrators mainly set out to modify the binary code of the application.[133] Another form of modification of information may be exercised by hacktivists or extremists through the defacement of websites.

---

[128] Krebs, Brian. 2015a. 'Online cheating site Ashley Madison hacked.' *KrebsonSecurity*, July 15. As of 12 October 2015: http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/
[129] Geuss, Megan. 2015. 'Paying $20 to delete your Ashley Madison profile was probably a bad idea.' *Arstechnica*, July 10. As of 12 October 2015: http://arstechnica.com/business/2015/07/cheaters-hook-up-site-ashley-madison-makes-account-deletion-confusing/
[130] CNN Money. 2015. 'Adult dating site hack exposes sexual secrets of millions.' *CNN*, May 22. As of 12 October 2015: http://money.cnn.com/2015/05/22/technology/adult-friendfinder-hacked/
[131] Geuss 2015.
[132] Krebs 2015a.
[133] ENISA 2015a, p. 7.

2.8.5 Denial of service

Denial of service attacks, more frequently identified as distributed denial of service (DDoS) attacks, are perhaps the most straightforward threat category. According to Verizon, the number of DDoS attacks increased during its most recent reporting year. Its reporting partners logged double the number of incidents in comparison to the previous year.[134]

In terms of the impact of DDoS attacks, the NCSC notes that DDoS attacks on DigiD – the Dutch digital identity mechanism – illustrate the type of impact such an attack can have on the entire supply chain as a result of extensive digitisation. During DDoS attacks that limited the availability of Digi-D in mid-2013, (semi-)governmental services became less accessible to citizens, as did healthcare institutions and insurers that also used the government-provided digital identity mechanism. This demonstrates that disruption of one critical aspect of a supply chain can negatively influence other critical processes leading to potential serious harm.[135]

According to the ACSC, perpetrators are increasingly finding ways to monetise activities that were previously considered to have solely a nuisance value. Profit-driven cybercriminals are also using DDoS to blackmail financial service providers into paying them to stop the attack. The Russian Central Bank even introduced a centre to cope with attacks on the financial services sector.[136] As Lewis (2015) notes, 'What once began as an attacker defacing a website, later graduated to launching DDoS attacks. Now, those very attackers have demonstrated that they are no longer satisfied with press exposure. Now we see evidence of attacks being launched for money.'[137] Lewis describes the DDoS for BitCoin (DD4BC) crew, which he first discovered in 2014 when they began trial run attacks on a number of websites. According to Lewis, DD4BC demanded 'a paltry sum' from their victims, indicating they were just 'kicking their tires on their new machine'. DD4BC, and others who copy their methods, begin the attack by launching a small burst of requests at the victim's website before emailing the victim to suggest they take a look at their logs. This is to demonstrate the capability of the crew and is a prelude to asking for money. If the victim fails to comply, either the attack continues or perpetrators begin destroying data (see Section 2.8.2). This type of threat is global, ranging from Hong Kong[138] to Finland[139] to the US.[140]

However, DDoS attacks are also carried out by other actors, namely hacktivists. The ACSC describes how 'a major Australian organisation was the victim of a sustained DDoS targeting its main website. An issue-motivated group purporting to oppose the work of this organisation claimed responsibility for the activity. The group had exploited poorly configured domain name system (DNS) infrastructure to conduct the activity.'[141]

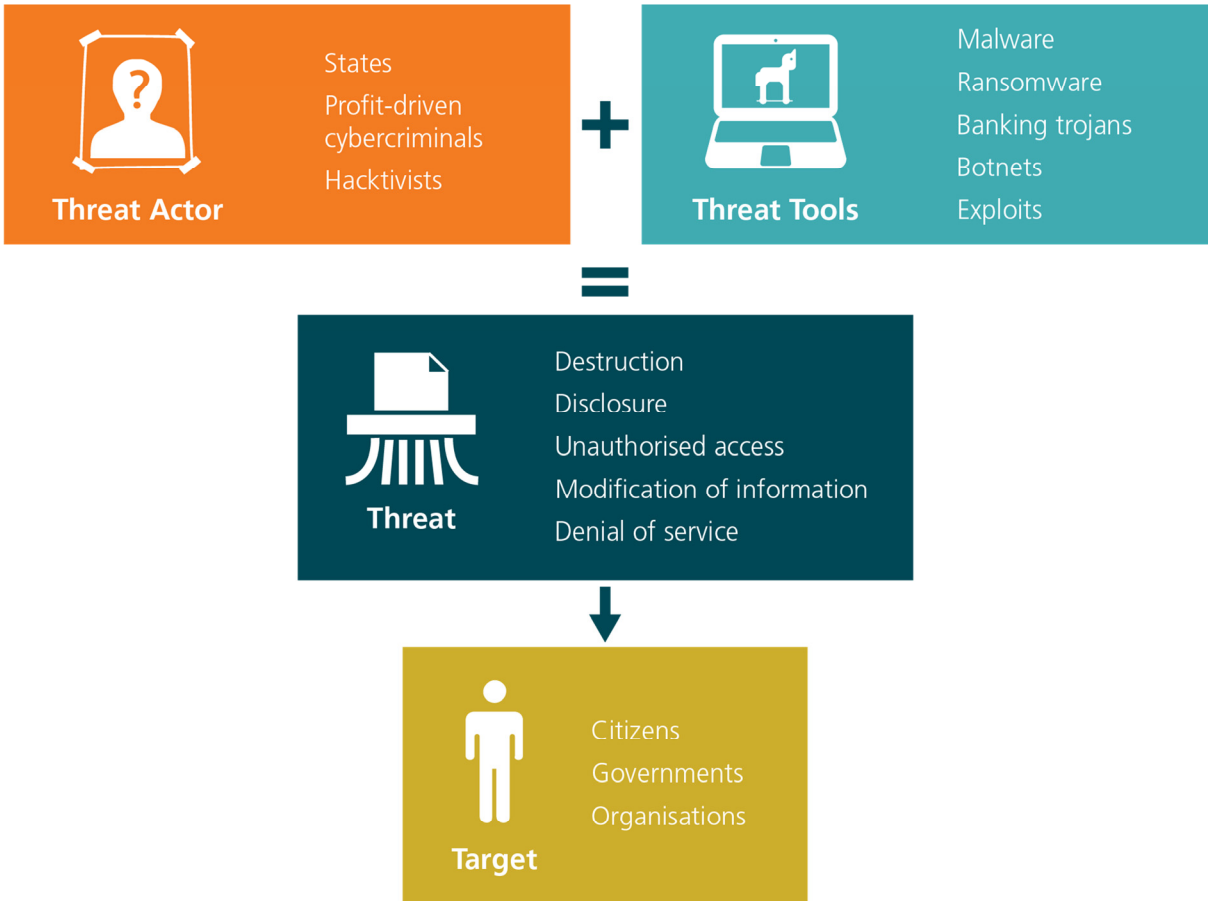
---

[134] Verizon 2015.
[135] NCSC 2014.
[136] Rains, Tim. 2013. 'Ransomware is on the Rise, Especially in Europe.' *Microsoft Blog*, November 19. As of 12 October 2015: http://blogs.microsoft.com/cybertrust/2013/11/19/ransomware-is-on-the-rise-especially-in-europe/
[137] Lewis, Dave. 2015. 'DDoS attacks have graduated to extortion.' *Huffington Post*, June 23. As of 12 October 2015: http://www.huffingtonpost.com/dave-lewis2/ddos-attacks-have-graduat_b_7639516.html
[138] Young, Joseph. 2015a. 'Hong Kong banks targeted by DDoS attack.' *BitCoinMagazine*, May 18. As of 12 October 2015: https://bitcoinmagazine.com/20449/hong-kong-banks-targeted-ddos-attacks-bitcoin-payout-demanded/
[139] Drinkwater, Doug. 2015. 'Finnish bank hit by DDoS attacks.' *SC Magazine UK*, January 8. As of 12 October 2015: http://www.scmagazineuk.com/finnish-bank-hit-by-ddos-attacks/article/391591/
[140] FBI. 2015a. 'Private Industry Notification.' As of 12 October 2015: https://info.publicintelligence.net/FBI-BitcoinExtortionCampaigns.pdf
[141] ACSC 2015.

2.9 Threats: from actors and tools to targets

Despite the challenges associated with existing threat assessments, important insights about the threat landscape can still be generated from available data when caveats are taken into consideration. This section illustrates how the threat components – actors, tools and targets – connect with each other to form a threat landscape. Figure 4 summarises the findings from the six threat assessments, identifying key categories in each component and demonstrating how actors employ certain cybertools to pose threats against their targets.

Figure 4. Threat components: actor, tools and targets



Source: RAND Europe study team

2.10 Questioning the severity of cyberthreats

This mapping exercise in the previous section identified key threat actors and tools in relation to the threats in the cyber domain. However, it did not attempt to assess the relative importance of each actor, tool or threat, which is crucial for any policy decision. It also did not suggest whether such threat components are becoming more or less pertinent over time. Due to the incompatibilities of definitions, metrics and approaches, weighing the severity of threats on the basis of existing threat assessments is rendered infeasible (see Section 2.3).

A systematic review of whether threat severity is increasing or decreasing is also complicated by a possible tendency for cyberthreats to be inflated.

2.10.1 Threat inflation as a result of method

Eric Jardine, along with other experts in the field, argues that the level of security in cyberspace is far better than most believe, once the indicators are expressed in proportion to the growing size of the Internet.[142] He explains:

> *Since cyberspace is, in a number of ways, expanding at an exponential rate, it is reasonable to expect that the absolute number of cyberattacks will also increase simply because the Internet ecosystem is getting bigger and not necessarily because the situation is growing worse.*[143]

Jardine therefore compares the absolute numbers to their normalised counterparts on three modalities of cybercrime – vectors, occurrence and costs. He uses proxy indicators to represent the size of the Internet: number of Internet users, websites and web domains for vectors; number of email users, internet users and volume of Internet traffic for occurrence; and the size of Internet's contribution to global GDP for costs.

Once normalised, the findings paint a more favourable picture of the current level of cybersecurity, while absolute numbers inflate the threat.[144] For instance, Jardine demonstrates that between 2008 and 2014 the number of new vulnerabilities increased in absolute terms by 17.75 per cent. When normalised around the number of Internet users, however, the number of new vulnerabilities in fact declined by 37.13 per cent during that period.[145] Another interesting observation is that while both the absolute and relative numbers indicate improvements on botnets, the normalised trends show a faster rate of improvement.[146] A comparable discussion has taken place in the past about the reliability of quantifying the cost of cybercrime.[147]

2.10.2 Threat inflation through rhetoric

Different research approaches can lead to drastically different conclusions about the severity of cyberthreats. This explains the current scepticism among experts and researchers about the ways in which cybersecurity threats are portrayed. According to Thierer, 'The rhetorical device most crucial to all technopanics is "threat inflation."'[148] Thierer borrows the term 'threat inflation' from Cramer & Trevor, who define it as 'the attempt by elites to create concern for a threat that goes beyond the scope and urgency that a disinterested analysis would justify'.[149] Thierer mentions specific phrases or concepts used to appeal to such fear and to inflate cyberthreats. Examples are a 'cyber Pearl Harbor', 'cyberwar', 'cyber Katrina' and 'cyber 9/11'.

---

[142] Jardine, Eric. 2015. 'Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime.' *Global Commission on Internet Governance*, No. 16. As of 12 October 2015: https://www.cigionline.org/sites/default/files/no16_web_0.pdf
[143] Jardine 2015, p. 2.
[144] Jardine recognises that the conclusions drawn from this study must be qualified in light of the poor quality of existing data. But he stresses that while the figures might be skewed, 'they are definitely more accurate than the simple absolute figures'.
[145] Jardine 2015, p. 9.
[146] Jardine 2015, p. 12.
[147] Anderson, Ross et al. 2012. 'Measuring the Cost of Cybercrime.' In the *Workshop on the Economics of Information Security*. As of 12 October 2015: http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf
[148] Thierer, Adam. 2013. 'Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle.' *Minnesota Journal of Law, Science and Technology* 14(1): 309-386
[149] Thierer 2013, p. 317.

2.10.3 Threat inflation through media coverage

Thierer notes that certain incidents travel from the discoverer to the media to be used as 'evidence' of the seriousness of the threat; these incidents then inform public and political discourse about the need to take a particular action. When actual incidents are inspected more closely, however, details are often different. Aspects of a particular event that the media portray as facts are either embellished or simply untrue. Thierer describes an example in the US, but similar events also occur in other countries. Yet, the commotion caused in the media by policy makers often induces action. Board members and government officials acquiesce due to the fear of potential reputation damage.[150]

2.11 Threat vectors

Besides discussing current trends, threat assessments can also provide predictions about the future and potential innovative threats – or to put it more accurately, threat vectors. While these were not included in the mapping, two vectors in particular are worth elaborating on, based on the threat assessments reviewed in this study. The first is the Internet of Things (IoT). According to some experts, attacks on the IoT will in the future transform from proof-of-concept to a regular risk.[151] So far – as far as is publicly known – these have remained limited. Lyne writes: 'Perhaps the reason the Internet of Things has been less exploited so far is cyber criminals have yet to find a business model that enables them to make money.'[152] Nonetheless, expectations are that this will change in the near future and that the IoT will introduce multiple new attack vectors due to the increase in the number of connected objects and the correlating surge of data that need to be protected.

Another frequently discussed threat vector is mobile phones. Verizon, however, comes to a 'data-driven conclusion' that mobile devices are not a preferred vector in data breaches.[153] They support this conclusion by stating that 'an average of 0.03 per cent of smartphones per week – out of tens of millions of mobile devices on the Verizon network – were infected with "higher-grade" malicious code"'.[154] Even so, the German Ministry of the Interior notes, 'Since mid-2013 underground forums have been offering malware for monitoring and manipulating android smartphones. The malware was used for such purposes as attacks on online banking transactions using mTANs.'[155] Europol also describes how malicious applications could spoof legitimate mobile banking applications as a means to steal log-in credentials. Yet, since the application is on the mobile phone, it can also intercept the Mobile Transaction Authentication Number (mTAN), as testified to by the German Ministry of the Interior. The use of a two-factor authentication becomes ineffective since both parts of the authentication process are accessible via a single device. This threat has been identified previously.[156] Europol also describes how smartphones have become attractive targets for ransomware. The first samples of mobile-focused ransomware came out in 2013.

---

[150] Libicki, Martin C., Lilian Ablon & Tim Webb. 2015. *Defender's Dilemma: Charting a Course Toward Cyber Security*. Santa Monica, Calif.: RAND Publications. As of 12 October 2015: http://www.rand.org/pubs/research_reports/RR1024.html

[151] See for example: Pescatore, John. 2014. *2014 Trends That Will Reshape Organizational Security*. As of 12 October 2015: https://www.sans.org/reading-room/whitepapers/analyst/2014-trends-reshape-organizational-security-34625

[152] Lyne, James. 2015. *Security Threat Trends 2015.*Sophos. As of 12 October 2015: https://www.sophos.com/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf, p. 2

[153] Verizon 2015.

[154] Verizon 2015, p. 19.

[155] BSI 2014.

[156] Van der Meulen 2011b.

2.12 Conclusion

The different meanings of a term that is used as frequently as 'threat', especially in the context of cybersecurity, introduce challenges. A clear and universally accepted definition of what constitutes a threat, at least within the context of cybersecurity, could allow a more comprehensive delineation of what threat assessments should include and exclude, or at least how to classify the different components. Developing a clear definition can also allow the concept of threat to be operationalised and help distinguish between threats and other related concepts. As indicated in Section 1.3, the challenge is that cybersecurity itself has different connotations depending on the stakeholder's interest, rendering what constitutes a 'threat' subjective.[157] Threats therefore cannot be identified and discussed in isolation; contextual elements must be discussed in tandem to ensure an understanding of how different variables interact.

The breakdown of threat components in this chapter aims to demonstrate the variables that exist and to explore how the identification of a threat to a specific target requires the incorporation of all these variables. This is not a comprehensive overview, due to its reliance on existing threat analyses and the fundamental differences in how they have been carried out by different entities.

To map the cyberthreat landscape, actors, tools and threats are distinguished and the frequency and nature of their coverage in six threat assessments reviewed.

- The study identifies and categorises states, profit-driven cybercriminals and hacktivists and extremists as threat actors.
- Threat tools like malware and its variants such as (banking) Trojans, ransomware, PoS malware, botnets and exploits are explained.
- The five categories of threat described in this chapter include unauthorised access, destruction, disclosure, modification and denial of services.

The study team noted whether and how many times a threat component is mentioned in each threat assessment and followed this with a detailed description of its particularities.

Finally, this chapter highlights varying perceptions of the severity of the threats identified and introduces the concept of 'threat inflation'.

[157] Dunn Cavelty 2013a.

3 CYBERSECURITY CAPABILITIES IN THE EUROPEAN UNION

KEY FINDINGS

- EU cybercapabilities currently focus on three areas that are identified as top objectives in the European Union Cyber Security Strategy: cyberresilience, cybercrime and cyberdefence.
- The European Union Agency for Network and Information Security (ENISA) plays a central role in achieving cyberresilience. ENISA's authoritative status signifies the EU's strategy to identify gaps in Member States' cybersecurity capabilities and facilitate bridging those gaps through operational support.
- Another product of EU's harmonisation measures is the creation of a common European cybercrime platform, the European Cyber Crime Centre (EC3).
- Where national security is concerned, the EU measures have been less pronounced; therefore, the cyberdefence domain in the EU appears less proactive. Traditional approaches to pan-European defence policy may be unsuitable given the boundless character of cybersecurity threats.

3.1 Background to EU cybercapabilities

The cybercapabilities discussed in this chapter are not comprehensive, but instead, focus on core EU agencies dedicated to cybersecurity. In describing the role of each organisation, this chapter will highlight the ongoing discussions surrounding the Network and Information Security (NIS) Directive and how this may impact the organisations currently involved in cybersecurity in the European Union (EU).

3.1.1 The EU Cyber Security Strategy

The European Commission introduced the EU Cyber Security Strategy (the Strategy) in 2013.[158] As outlined in its introduction, three broad motivations drive the Strategy. The first is economic: EU prosperity is increasingly dependent on the strength of its information and communication systems and growth is not viable without an 'open, safe, and secure cyberspace'. The second motivation concerns its political aims: to design properly and adopt a multi-stakeholder model of governance that seals the European capability gap in cybersecurity. The third is ideational: the norms and principles that protect fundamental rights, democracy and the rule of law in the EU must apply equally to its cyberspace.

While these motivations are not unique to the EU, they have particular policy implications given the wide-ranging discrepancies in the cybercapabilities of its Member States. Therefore, one overarching theme in the Strategy is the emphasis on harmonisation and coordination to overcome the currently fragmented approaches of Member States. This has manifested in various efforts: establishing pan-European cyber agencies, strengthening cyberrelated legislation and helping Member States to enhance their domestic capabilities. The challenge is to ascertain the appropriate margins of power to be delegated to domestic authorities, while implementing a coordinated European cybersecurity agenda.

[158] European Commission. 2013a. *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cyberstrategy of the European Union: An Open, Safe and Secure Cyberspace*. JOIN (2013) 1 Final. As of 12 October 2015: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Given the principal theme of harmonisation and coordination, the Strategy has five objectives: [159]

1. Achieving cyberresilience.
2. Drastically reducing cybercrime.
3. Developing cyberdefence policies and capabilities related to the Common Security and Defence Policy (CSDP).
4. Developing the industrial and technological resources for cybersecurity.
5. Establishing a coherent international cyberspace policy for the EU and promoting core EU values.

Increased commitment to expanding industrial resources and collaboration with international stakeholders are critical, as they play an enabling role in achieving cyberresilience, reducing cybercrime and strengthening cyberdefence. The main focus of this chapter is on EU capabilities for the first three objectives; the last two are discussed only indirectly. Capabilities can be operationalised as 'the means to accomplish a mission, function, or objective'.[160] With this in mind, this chapter will outline the existing EU cybercapabilities for each of the first three objectives, relying exclusively on the literature and the ongoing policy debate as recorded by accessible policy documents.

3.1.2 The Network and Information Security Directive

Alongside the EU Cyber Security Strategy in February 2013, the European Commission proposed a Directive on Network and Information Security (the NIS Directive). The Directive seeks 'to ensure a high common level of network and information security across the EU'[161] by various means of regulation.

The core purpose of the Directive is to achieve minimum harmonisation. At the moment, under Chapter IV of the proposal for the NIS Directive, states are obliged to maintain a minimum level of national cybercapabilities. This entails designing and implementing national NIS strategies, setting up NIS competent authorities (or 'single points of contact') and instituting Computer Emergency Response Teams (CERTs). These entities must monitor the security and reporting requirements of their domestic private companies (or 'market operators') and collaborate with their European counterparts, namely the European Network and Information Security Agency (ENISA) and the European Union Computer Emergency Response Team (CERT-EU).

3.1.3 Areas of debate regarding the NIS Directive

The Directive has led to considerable discussion and debate. While all Member States acknowledge the need to act against cyberthreats, views differ significantly on how best to achieve network and information security. Implied in the proposed wordings of the Directive is the Commission's preference for legally binding measures. However, some Member States promote and prefer a flexible approach, where regulations are restricted

[159] European Commission 2013a, pp. 4–5.
[160] National Initiative for Cybersecurity Careers and Studies (NICCS). n.d. 'Explore Terms: A Glossary of Common Cybersecurity Terminology.' As of 12 October 2015: https://niccs.us-cert.gov/glossary#capability
[161] European Commission. 2013b. *Proposal for a Directive of the European Parliament and the Council – Concerning measures to ensure a high common level of network and information security across the Union*. COM (2013) 48 Final. As of 12 October 2015: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

to critical infrastructure protection and additional activities are executed on a voluntary basis.[162]

Some specific points of disagreement regarding the NIS Directive are elaborated further in Chapter 6. They include:

- The definition and scope of 'market operators'.
- The nature of the cooperation framework.
- The requirement for national NIS strategies and competent bodies, particularly in relation to incident notification.[163]

These issues have appeared in discussions in both the European Parliament (EP) and the Council of the European Union (the Council). On 13 March 2014, the EP adopted, in its first reading, a legislative resolution and 138 amendments on the proposal: it went through substantial changes and the EP's support was convincing thereafter, as the resolution passed by 521 votes to 22, with 25 abstentions.[164] One crucial change concerned the scope of the Directive: 'public administrations' and 'market operators' were relieved of obligatory common minimum security requirements and an explicit exemption was also made for hardware and software providers.[165] Emphasis was placed on the use of existing domestic structures and compliance with other EU requirements (i.e. data protection laws) to fulfil the aims of the Directive. Some amendments reflected clarifications or elaborations: for instance, the term 'competent authorities' was replaced by 'single points of contact' and definitions of 'risk', 'incident' and 'operators of critical infrastructure' were expanded.

While no consensus has emerged on the Council's position on the proposal, exploratory trilogues with the EP have begun regarding main principles and general orientations, such as scope, cooperation framework and incident notification.[166] The debate about scope concerns definitional boundaries of its three elements: 'operators', 'essential services' and 'specific sectors' (to be identified in Annex II of the proposal). According to the memo drafted in preparation for the first exploratory trilogue, '[v]iews appear to be converging that operators – be they private or public – providing essential services in specific sectors (Article 3(8)) should be subject to the operative provisions in the Directive (in particular Article 14, which deals with incident notification)'.[167] What must be included in each element is still heavily debated. Similarly, discussions on security requirements and incident notification surround the exact modalities of mandatory notification. A cooperative framework is also under development: the strategic aims of an EU-wide cooperation group and the operational tasks of CERTs require refinement.

[162] Shooter, Simon. 2014a. 'MEPs vote strongly in favour of the proposed European Cybersecurity Directive.' *Bird & Bird*, March 13. As of 12 October 2015: http://www.lexology.com/library/detail.aspx?g=c39213ca-77b0-432e-943e-37854fc6b921
[163] European Parliament 2013b.
[164] Shooter et al. n.d.
[165] European Parliament. 2014a. *Legislative resolution of 13 March 2014 on the 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*. P7_TA(2014)0244, (COM (2013)0048 – C7-0035/2013 – 2013/0027(COD)). As of 12 October 2015: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0244&language=EN
[166] Council of the European Union. 2014c. *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 - Preparations for the 1st informal exploratory trilogue*. ST 14076 2014 INIT, October 8. As of 12 October 2015: http://data.consilium.europa.eu/doc/document/ST-14076-2014-INIT/en/pdf
[167] Council of the European Union. 2014. 2013/0027 (COD).

3.2 Achieving cyberresilience

The Digital Agenda for Europe (the Agenda)[168] is one of the seven flagship initiatives of the Europe 2020 Strategy,[169] the all-embracing purpose of which is to achieve 'smart, sustainable and inclusive growth'. Besides its ambition for a digital single market, the Agenda aims to address the lack of trust and security in cyberspace.[170] In fact, the goals enshrined in Pillar III are directly aligned with the Strategy's objectives on cyberresilience and cybercrime. The Agenda lays out a list of actions and tracks the status of various measures undertaken so far. The overarching emphasis has been on building resilience. The relevant actions include (but are not limited to):[171]

- Action 28: Reinforced NIS policy
- Action 33: Support EU-wide cybersecurity preparedness
- Action 38: Member States to establish pan-European CERTs
- Action 41: Member States to set up national alert platforms
- Action 123: Proposal for NIS Directive.

3.2.1 ENISA to facilitate enhanced cyberresilience in the EU

In accordance with its mandate, ENISA plays a leading role in facilitating enhanced cyberresilience in the EU, especially with respect to reducing capability gaps among the Member States. ENISA was originally created on 10 March 2004 [172] as a purely complementary entity to help prevent, address and respond to network information and security problems in the EU. The agency has since undergone various changes. The duration of its mandate was extended in 2008[173] and 2011.[174] When the Framework Directive of 2002 [175] was amended in 2009, [176] the boundaries of ENISA's mandate expanded significantly: 'The Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical implementing measures with a view to

[168] European Commission. n.d.-a. 'Pillar III: Trust & Security.' *Digital Agenda for Europe*. As of 12 October 2015: http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security
[169] European Commission. n.d.-b. 'Digital Agenda in the Europe 2020 Strategy.' *Digital Agenda for Europe*. As of 12 October 2015: http://ec.europa.eu/digital-agenda/en/digital-agenda-europe-2020-strategy
[170] European Commission. n.d.-a.
[171] European Commission. n.d.-a.
[172] European Commission. 2004. 'Establishment of the European Network and Information Security Agency.' Regulation (EC) no. 460/2004. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004R0460
[173] European Parliament and Council of the European Union. 2008. *Amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration*. Regulation (EC) no. 1007/2008, 24 September. As of 12 October 2015: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF
[174] European Parliament and Council of the European Union. 2011. *Amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration*. Regulation (EU) No 580/2011, 8 June. As of 12 October 2015: https://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1
[175] European Parliament and the Council of the European Union. 2002. *Common regulatory framework for electronic communications networks and services (Framework Directive)*. Directive 2002/21/EC, 7 March. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0021
[176] European Parliament and Council of the European Union. 2009. *Amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services*. Directive 2009/140/EC, 25 November. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0140

harmonizing measures'.[177] In effect, ENISA was endowed with the authority to enforce, as its advice formed the core of the Commission's harmonisation strategy.

Other vital responsibilities of ENISA are featured in the new Basic Regulation of 2013.[178] As a body of expertise, its main tasks are to advise the Commission and Member States on NIS-related issues, collect and analyse data to identify emerging risks, promote risk assessment and management, and encourage cooperation among various stakeholders, in particular by fostering public-private partnerships.[179] In fact, due to the nature of cyber vulnerabilities – boundless and (arguably) ungovernable – building resilience and mitigating risks necessitate a multi-stakeholder approach. In this respect, ENISA enhances information sharing among various actors by acting as an expert *intermediary*, assessing capabilities, identifying gaps and shaping policies at national and European levels.

3.2.2 CERTs as implementers of the NIS Directive

CERTs play a vital role in cyberresilience more generally but this section focuses on their role as implementers of the NIS Directive. As the success of the proposed NIS Directive depends not only on its approval and subsequent adoption but also on its implementation, CERTs, or Computer Security and Incident Response Teams (CSIRTs), are tasked to implement the requirements introduced as a result of the NIS Directive, once approved.

CERTs or CSIRTs are entities that respond to information security incidents and provide primary security services such as alerts, warnings, advice and training.[180] CERTs came into existence after the 'Morris Incident' in the late 1980s during which a worm, a form of malware, subverted the global information technology (IT) infrastructure, causing massive damage.[181] Soon after, in 1992, the first European CERT, SURFnet-CERT3, was created by the Dutch company SURFnet.[182] Today, according to ENISA's inventory of CERT activities in Europe, there are more than 100 known CERTs operating.[183]

To embed a culture of threat anticipation and rapid response, the Directive requires each Member State to institute a national CERT, which would 'act as security point of contact'.[184] To that end, ENISA helps facilitate the set-up and running of CERTs,[185] collecting and sharing best practices and brokering the exchange of information beyond Europe with international players such as Task Force CSIRT (TF-CSIRT), US-CERT and Asian-Pacific-CERT.[186] CERT-EU was created following a year-long pilot to strengthen operational resilience to incidents and threats against wider European networks. While

[177] European Parliament and Council of the European Union 2009.
[178] European Parliament and Council of the European Union. 2013b. *Concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004*. Regulation (EU) no. 526/2013, May 21. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0526
[179] European Union Agency for Network and Information Security (ENISA). 'What does ENISA do?' As of 12 October 2015: http://www.enisa.europa.eu/about-enisa/activities
[180] ENISA. 2015b. 'CERT.' As of 12 October 2015: http://www.enisa.europa.eu/activities/cert
[181] ENISA. 2006. *CERT Cooperation and its Further Facilitation by Relevant Stakeholders*. As of 12 October 2015: https://www.enisa.europa.eu/activities/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders/at_download/fullReport
[182] ENISA 2006.
[183] ENISA 2015c. 'CERT Inventory.' As of 12 October 2015: http://www.enisa.europa.eu/activities/cert/background/inv
[184] ENISA 2006, p. 9.
[185] ENISA. 2015b. 'CERT.' As of 12 October 2015: http://www.enisa.europa.eu/activities/cert
[186] ENISA. 2015d. 'CERT Factsheet.' As of 12 October 2015: http://www.enisa.europa.eu/activities/cert/background/cert-factsheet

the scope of CERT-EU's activities covers the security lifecycle – prevention, detection, response and recovery – a particular focus area of the CERT-EU is in 'building on and complementing the existing capabilities in the constituents'.[187] Funded by major European institutions such as the European Commission, the Council and the EP, CERT-EU operates under the strategic guidance of an inter-institutional steering board.[188] On 25 February 2015, the steering board agreed on a new mandate for CERT-EU concerning its service catalogue and the information-sharing framework, seeking to strengthen ties with the community of CERTs and IT security companies housed in the Member States and elsewhere.[189]

3.3 Reducing cybercrime

The second objective outlined in the Strategy is combatting cybercrime. This has been emphasised on multiple occasions.[190] The Agenda's action points under Pillar III emphasise the importance of fighting cybercrime[191]:

- Action 30: Establish a European cybercrime platform.
- Action 31: Analyse the usefulness of creating a European cybercrime centre.
- Action 32: Strengthen the fight against cybercrime and cyberattacks at international level.

Before looking at the more recent developments in countering cybercrime at the EU level, this section reflects briefly on the Council of Europe (CoE) Convention on Cybercrime, also known as the Budapest Convention.[192] As a binding international treaty that compels a 'common criminal policy' against cybercrime, by coordinating national legislation and law enforcement and fostering international cooperation, the Budapest Convention has been a pioneer in the area of cybercrime legislation, especially with respect to providing the legal framework to facilitate the countering of cybercrime.[193] The Strategy seeks to achieve ratification of the Budapest Convention by all Member States by December 2015.

The Convention specifies four computer-related crimes: infringements of copyright, fraud and forgery, child pornography and network security breaches such as hacking and illegitimate data interception.[194] By defining these criminal offenses, the Convention aids its parties in adopting appropriate laws and procedures to respond to them; the parties

[187] CERT-EU. 2013. 'RFC 2350.' As of 12 October 2015: http://cert.europa.eu/static/RFC2350/RFC2350.pdf
[188] European Commission. 2012a. 'Cyber security strengthened at EU institutions following successful pilot scheme.' *Press Release,* September 12. As of 12 October 2015: http://europa.eu/rapid/press-release_IP-12-949_en.htm
[189] Council of the European Union. 2015a. *EU Cybersecurity Strategy: Road map development*. As of 12 October 2015: http://www.statewatch.org/news/2015/apr/eu-council-cyber-security-roadmap-6183-rev1-15.pdf
[190] Europol's Serious and Organised Crime Threat Assessment of 2013 designated cybercrime as an 'increasing threat to the EU in the form of large-scale data breaches, online fraud and child sexual exploitation'. Moreover, the 'Strategic guidelines for justice and home affairs' in 2014 outlined curtailing cybercrime as central to modernising the EU security strategy. See: Council of the European Union. n.d. 'Strategic guidelines for justice and home affairs.' As of 12 October 2015: http://www.consilium.europa.eu/en/policies/strategic-guidelines-jha/
[191] See: European Commission. n.d.-a.
[192] Council of Europe. 2001. 'Convention on Cybercrime (Budapest Convention).' As of 12 October 2015: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
[193] Archick, Kristin. 2002. *Cybercrime: The Council of Europe Convention*. Congressional Research Service. As of 12 October 2015: http://digital.library.unt.edu/ark:/67531/metacrs2394/m1/1/high_res_d/RS21208_2002Apr26.pdf
[194] Keyser, Mike. 2003. The Council of Europe Convention on Cybercrime. *Journal of Transnational Law and Policy* 12(2): 287-326

are 'granted great latitude with respect to the legislative approach'.[195] Further, the Convention lays down principles of extradition, mutual assistance and 'spontaneous information' (which entitle parties to receive relevant data without a prior request) with the aim of effecting vigorous cross-border cooperation.[196] These principles are then operationalised through Article 35, which institutes a '24/7 network': it requires each party to establish a point of contact that is available 24 hours a day, seven days a week.[197] This is considered of utmost importance to improving law enforcement against cybercrime, which is inherently transnational. At the time of writing, three Member States have not ratified the Convention: Greece, Ireland and Sweden.[198]

3.3.1 EC3 as the centre of EU cyberintelligence

This norm-setting, cooperative approach is echoed at the EU level. The 2013 Directive on attacks against information systems, which replaces the Council Framework Decision of 2005,[199] sets out two objectives: 1) setting minimum standards for defining criminal offences and corresponding sanctions; and 2) advancing cooperation between domestic law enforcement agencies and specialised Union bodies, namely Europol (or more specifically EC3), Eurojust and ENISA.[200] With regard to standardising criminal offences, the Directive introduces four common categories of offence: illegal access to information systems, illegal system interference, illegal data interference and illegal interception.[201] Particular attention has also been given to the introduction of criminal penalties against botnets. In relation to enhancing cooperation, the Directive emphasises the significance of making points of contact available in each Member State and reinforces the need to equip Europol and ENISA with relevant information. EC3 is the centre of EU cyberintelligence.

Established within Europol in 2013, the EC3 has been tasked with focusing on cybercrimes that are committed by organised groups, affect critical (information) infrastructure or cause serious harm to the victim.[202] Its operations are threefold. First, *Focal Point Terminal* investigates international payment fraud, collaborating with key institutions such as the European Central Bank (ECB) and national banks by giving real-time access to its information databases and forensic analyses.[203] Second, *Focal Point Cyborg* combats high-tech crimes against critical infrastructure sectors. Cyborg employs the Europol Malware Analysis System (EMAS) to support forensic examination of such crimes and supports Joint Investigation Teams (JITs) to tackle high-profile transnational operations (i.e. botnets).[204] Third, *Focal Point Twins* focuses on child sexual exploitation.[205]

---

[195] Keyser 2003, p. 300.
[196] Keyser 2013, p. 318.
[197] Keyser 2013, p. 321.
[198] Council of Europe. 2015a. 'Convention on Cybercrime: status as of 24/8/2015.' As of 12 October 2015: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
[199] European Parliament and Council of the European Union. 2013a. *On attacks against information systems and replacing Council Framework Decision 2005/222 JHA*. Directive 2013/40/EU, 12 August. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32013L0040
[200] European Parliament and Council of the European Union. 2013a.
[201] European Parliament and Council of the European Union. 2013a.
[202] Europol. 2015a. 'Combating cybercrime in a digital age.' As of 12 October 2015: https://www.europol.europa.eu/ec3
[203] Europol. 2015b. 'Payment fraud.' As of 12 October 2015: https://www.europol.europa.eu/ec3/payment-fraud
[204] Europol. 2015c. 'High-tech crimes.' As of 12 October 2015. https://www.europol.europa.eu/ec3/high-tech-crimes
[205] Europol. 2015d. 'Child sexual exploitation.' As of 12 October 2015: https://www.europol.europa.eu/ec3/child-sexual-exploitation

An overarching feature of the EC3 operations is its cyberintelligence. Crucially, this analytic hub connects law enforcement authorities, CERTs, industries and academic communities, and builds a reliable source of intelligence on emerging threats.[206] Where identified threats are of high order and magnitude, the Joint Cybercrime Action Taskforce (J-CAT) brings in the expertise of various liaising authorities beyond the EU to coordinate an international response. J-CAT was launched on 1 September 2014 by EC3, the EU Cybercrime Task Force (EUCTF) the US Federal Bureau of Investigation (FBI) and the UK National Crime Agency (NCA).[207] It works on a case-by-case basis with the prerogative to prioritise or pursue an investigation on its terms.[208]

The EC3 also has a strategic function, intricately involved in strengthening its operations. Various services are provided. Through strategic analysis, EC3 offers comprehensive advice on emerging trends and methods of criminal activity to policymakers. [209] Moreover, it provides training to law enforcement authorities within and outside the EU, in collaboration with relevant entities such as the European Police College (CEPOL) and the European Cybercrime Training and Education Group (ECTEG). [210] Its forensic expertise also deserves attention: the EC3 created its own digital forensic laboratory, which delivers cutting-edge forensic assistance and leads its own independent technological research and development.[211] Other strategic tasks of EC3 include raising public awareness and widening partnerships in the international arena.[212]

3.3.2 From detection to prosecution: Eurojust

To fortify the judicial arm of European law enforcement, Eurojust was established in 2002 under a Council Decision.[213] The Decision was subsequently amended in 2003 to align its budgetary processes with the EU Financial Regulation[214] and again in 2009 to expand its mandate to fight transnational organised crime.[215] As an EU agency, Eurojust facilitates legal processes in cross-border investigations, in particular by supporting the implementation of international Mutual Legal Assistance (MLA) and extradition

[206] Europol. 2015e. 'Cyber intelligence.' As of 12 October 2015: https://www.europol.europa.eu/ec3/cyber-intelligence
[207] Europol. 2014b. 'Expert international cybercrime taskforce is launched to tackle online crime.' *Press Release*, September 1. As of 12 October 2015: https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime
[208] Europol. 2015f. 'Joint Cybercrime Action Taskforce (J-CAT).' As of 12 October 2015: https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat
[209] Europol. 2015g. 'Strategic analysis.' As of 12 October 2015: https://www.europol.europa.eu/ec3/strategic-analysis
[210] Europol. 2015h. 'Training and capacity building.' As of 12 October 2015: https://www.europol.europa.eu/ec3/training-and-capacity-building
[211] Europol. 2015i. 'Forensic expertise.' As of 12 October 2015: https://www.europol.europa.eu/ec3/forensic-expertise
[212] Europol. 2015j. 'Public awareness and prevention.' As of 12 October 2015: https://www.europol.europa.eu/ec3/public-awareness-and-prevention; Also see: Europol. 2015k. 'Outreach and cooperation.' As of 12 October 2015: https://www.europol.europa.eu/ec3/outreach-and-cooperation
[213] Council of the European Union. 2002. *Setting up Eurojust with a view to reinforcing the fight against serious crime*. Council Decision 2002/187/JHA, 28 February. As of 12 October 2015: http://eurojust.europa.eu/doclibrary/Eurojust-framework/ejdecision/Eurojust%20Decision%20(Council%20Decision%202002-187-JHA)/Eurojust-Council-Decision-2002-187-JHA-EN.pdf
[214] Council of the European Union. 2003. *Amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime*. Council Decision 2003/659/JHA, 18 June. As of 12 October 2015: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejdecision/2003%20Amendment%20to%20Eurojust%20Decision%20(Council%20Decision%202003-659-JHA)/Eurojust-Council-Decision-2003-659-JHA-EN.pdf
[215] Council of the European Union. 2009. *On the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime*. Council Decision 2009/426/JHA, 16 December. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009D0426

requests.[216] In fact, Eurojust has contact points in 23 non-Member States and works closely with the European Judicial Network (EJN), the European Anti-Fraud Office (OLAF) and Europol.

Eurojust's 2014 Annual Report highlights a number of its accomplishments in the cyber field.[217] The number of cybercrime cases for which Member States sought Eurojust's support increased by 14.5 per cent after 2013 and 122 Joint Investigative Teams (JITs) were assisted by Eurojust.[218] Eurojust participated in the Illegal Trade on Online Marketplaces (ITOM) project aimed at promoting a unified approach to illegal online trade in the EU. Further, Eurojust is associated with the Training of Trainers (ToT) programme, which seeks to bridge the gaps in understanding between law enforcement authorities and prosecutors. The programme also intends to harmonise the certification procedures for European cybercrime investigators.[219]

More notably, Eurojust is a founding member of the EUCTF, which was created in 2010 as a platform for exchanging best practices. The Task Force is made up of the heads of cybercrime units from all EU Member States, Europol, Eurojust and the Commission.[220] It was responsible for overseeing the piloting of J-CAT, the success of which has led to its full operationalisation. The EUCTF remains the high-level platform for synchronising EU actions against cybercrime.

By and large, an increasing focus on tackling cybercrime has been reflected in the growing concentration of the agencies, programmes and projects that exist for that purpose.

3.4 Fortifying cyberdefence

The third objective in the Strategy is developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP). Despite being a key priority listed in the Strategy, this particular aim has been approached separately from others that pursued more interactive measures. In fact, while a secure cyberspace is perceived as central to the successful implementation of the CSDP,[221] measures to improve cyberdefence have often been conducted independently from the broader strategy towards creating an 'open, safe and secure cyberspace'.[222] In part, this may be explained by the fact that defence and security have traditionally been domains of national competence in the EU. Measures to develop cyberdefence capabilities may therefore experience greater resistance in terms of harmonisation and coordination.

Despite the challenges, one noteworthy development in cyberdefence is the Cyber Defence Policy Framework, adopted by the European Council in 2014. In recognising

[216] Eurojust. 2015a. 'Mission and tasks.' As of 12 October 2015: http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx
[217] Eurojust. 2014a. 'Annual Report 2014.' As of 12 October 2015: http://www.eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202014/Annual-Report-2014-EN.pdf
[218] Eurojust 2014a.
[219] Eurojust 2014a.
[220] Drinkwater, Doug. 2014. 'EU's new cybercrime taskforce set to launch.' *SC Magazine UK*, July 21. As of 12 October 2015: http://www.scmagazineuk.com/eus-new-cybercrime-taskforce-set-to-launch/article/361822/
[221] Council of the European Union. 2014a. *Outcome of Proceedings – EU Cyber Defence Policy Framework*. As of 12 October 2015: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf
[222] European Commission. 2013a. *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cyberstrategy of the European Union: An Open, Safe and Secure Cyberspace*. JOIN (2013) 1 Final. As of 12 October 2015: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

cyberspace as a new domain of military activity, this document emphasises five priorities: 1) improving national defence capabilities of Member States related to CSDP; 2) increasing protection of CSDP communication networks; 3) promoting civil-military cooperation within wider EU cyber policies; 4) improving training, education and exercises; and 5) tightening international cooperation.[223] The purpose of this EU-wide cyberdefence policy is to address the capability gaps in Member States with respect to CSDP and to reinforce collaboration within Europe as well as with international players.

The European Defence Agency (EDA) supports the capability development necessary to implement the Strategy. The EDA came into being under a Joint Action of the Council of Ministers on July 12, 2004 'to improve European Defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future'.[224] The Joint Action was subsequently replaced by a Council Decision, formalising the EDA as an EU agency.[225] It was tasked with enhancing defence capabilities, promoting defence research and technology, encouraging cooperation on armaments, establishing a European Defence Equipment Market and developing a European Defence Technological and Industrial Base.[226] While it does not directly defend against cyberthreats, it facilitates capability development by promoting collaboration and launching relevant initiatives.

The EDA continues to improve the EU's cyberdefence capabilities, which were virtually non-existent before 2012.[227] It has accomplished ten cyberdefence projects in the last three years, spending roughly 10 per cent of its operational budget on cyberdefence.[228] To begin with, the EDA spearheaded research on technical cyberdefence requirements such as deployable Cyberdefence Situational Awareness Kits (OHQ/FHQ) and Advanced Persistent Threats (APT) detection systems. Further, the Agency inserted cyberdefence into the Pooling & Sharing agenda (2012), which invites ministries of defence to exchange information and share military capabilities on cyberdefence.[229] In December 2014, the EDA also facilitated Cyber Europe, a cybercrisis management exercise, to test the common crisis response platform.[230]

Another relevant project was a stocktaking study on the cyberdefence capabilities of EU bodies and Member States – an action item identified in EDA's Capability Development Plan of 2011.[231] According to this study, '[t]here is a complex operational setup regarding who undertakes cyberdefence activities (e.g. detection; reaction; response)

[223] European Defence Agency (EDA). 2015a. *Cyber Defence Factsheet*. As of 12 October 2015: https://www.eda.europa.eu/docs/default-source/eda-factsheets/2015-02-10-factsheet_cyber-defence
[224] EDA. 2015b. 'Mission.' As of 12 October 2015: http://www.eda.europa.eu/Aboutus/Whatwedo/Missionandfunctions
[225] Council of the European Union. 2011. *Defining the statute, seat and operational rules of the European Defence Agency and repealing Joint Action 2004/551/CFSP*. Council Decision 2011/411/CFSP, 12 July. As of 12 October 2015: https://www.eda.europa.eu/docs/documents/eda_council_decision.pdf
[226] EDA 2015b.
[227] Klimburg, Alexander. 2015. 'Here's Where Europe Has Made Big Changes in Cyber Security.' *DefenseOne,* February 3. As of 12 October 2015: http://www.defenseone.com/threats/2015/02/heres-where-europe-has-made-big-changes-cyber-security/104454/
[228] EDA 2015c. 'European Parliament Exchange of Views on Cyber Defence.' As of 12 October 2015: http://www.eda.europa.eu/info-hub/news/2015/03/18/european-parliament-exchange-of-views-on-cyber-defence
[229] EDA 2015c.
[230] Klimburg 2015. See also: European Commission. 2014. 'Biggest ever cyber security exercise in Europe today.' *Press Release*, October 30. As of 12 October 2015: http://europa.eu/rapid/press-release_IP-14-1227_en.htm
[231] Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle & Pablo Rodriquez. 2013. *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)*. Santa Monica, Calif.: Rand Corporation.

between the EEAS, General Secretariat of the EU Council, and European Commission'.[232] This finding highlights the need for EU cyberdefence policies to be streamlined and harmonised. Moreover, the study analyses capability information using the Defence Lines of Development (DLoDs), which recognise seven functional contributors to defence capability: doctrine, organisation, training, materiel, leadership, facility and interoperability. Of these, the study concludes that facilities (e.g. physical infrastructure specialised in cyberdefence missions) represent the most severe capability gap experienced across the EU.[233] This implies an increasingly important role for the EDA and, generally, a call for a more proactive EU stance on cyberdefence matters.

Having outlined the most prominent developments in cyberdefence, it is worth recalling that foreign and defence policies remain strictly outside the remits of the EP Committee on Civil Liberties, Justice and Home Affairs (LIBE) (which has commissioned this study). Indeed, where national security is concerned, the EU measures have been less pronounced. Conventionally, Member States have been reluctant to clarify the ambitions of CSDP for reasons of strategic imperative.[234] This explains, in large part, why the cyberdefence domain is seemingly less proactive. That said, however, the traditional approach to pan-European defence policy may be unsuitable given the boundless character of cybersecurity threats. As Howorth notes: 'The problem is that it is essentially a handful of the same EU Member States which are actively engaged in European initiatives, while the majority nod their agreement.'[235] This relates to the existing capability gap among the Member States, which broadly reflects the level of priority they assign to cyberdefence. Howorth continues: 'For Pooling & Sharing to be effective, significant transfers of sovereignty will have to be agreed.'[236]

3.5 Overview of EU cybercapabilities

Table 5 illustrates the overlaps in agencies' objectives. It shows that agencies with specific cybercrime and cyberdefence tasks simultaneously and, in many cases, necessarily play a role in strengthening cyberresilience.

Table 5. EU cybercapabilities with respect to cyberresilience, cybercrime and cyberdefence

EU cybercapabilities	Cyberresilience	Cybercrime	Cyberdefence
European Union Agency for Network and Information Security (ENISA)	**Advises** the Commission and Member States on issues related to network and information security **Promotes** risk assessment and management **Encourages** multi-stakeholder cooperation **Facilitates** setting up national CERTs		
European Cyber	**Plays** a strategic role	**Tasked** to reduce	

[232] Robinson et al. 2013.
[233] Robinson et al. 2013.
[234] Howorth, Jolyon. 2012. 'European defense policy needs recalibration.' *Foreign Policy*, June 29. As of 12 October 2015: http://foreignpolicy.com/2012/06/29/european-defense-policy-needs-recalibration/
[235] Howorth 2012.
[236] Howorth 2012.

Crime Centre (EC3)	by raising public awareness, leading technological research and development **Widens** partnerships in the international arena **Provides** cyberintelligence and connects law enforcement authorities, CERTs, industries and academic communities to build intelligence on risks and emerging threats	cybercrime committed by organised groups, affecting critical information infrastructure, or causing serious harm to the victim ***Joint Cybercrime Action Taskforce (JCAT)*** **Uses** the expertise of various liaising authorities within and beyond the EU to coordinate high-profile international investigations	
EUROJUST	**Trains** law enforcement authorities and prosecutors to harmonise cybercrime investigation procedures	**Facilitates** legal processes in cross-border cybercrime investigations, by supporting implementation of international MLA and extradition requests	
National Computer Emergency Response Teams (CERTs)	**Respond** to information security incidents and provide primary security services such as warnings, advice and training		
European Union Computer Emergency Response Team (CERT-EU)	**Prepares** for and responds to cyberattacks on EU institutions; facilitates exchanges of good practices		
European Union Cybercrime Task Force (EUCTF)	**Serves** as a platform for exchanging best practices		
European Defence Agency (EDA)	**Tasked** with enhancing defence capabilities; promotes defence research and technology **Encourages** cooperation on armaments **Participates** in exchange of best practices and facilitates EU-wide exercises on cybercrisis management		**Develops** common crisis response platform against cyberattacks

3.6 Conclusion

The efforts to strengthen EU cybercapabilities reflect the EU's determination to become a front-runner in the realm of cybersecurity, via the adoption of the EU Cyber Security Strategy in 2013. At the time of writing discussions about the proposed NIS Directive are

still continuing, with the positions of the Commission, the EP and the Council somewhat differing; consensus has yet to be reached.

Central to the Strategy is increasing cyberresilience, whether generally in terms of prevention, detection, response and recovery capabilities, or more specifically within the domains of cybercrime and cyberdefence. Various cyber agencies tasked with these objectives still play their part in strengthening the overall cyberresilience of the EU.

In terms of resilience, as it now stands (pending implementation of the NIS Directive), ENISA focuses primarily on advising the Member States and the Commission in formulating appropriate policies and undertaking actions at the national and European levels. This is facilitated by collaboration with various stakeholders such as the private sector and specialised agencies. Particularly important among ENISA's many activities is its focus on instituting and strengthening CERTs in Member States, while coordinating response activities at the EU level through CERT-EU. This demonstrates the EU's strategy of identifying gaps in Member States' cybersecurity capabilities and facilitating the bridging of those gaps through operational support.

Next to resilience building, the EU has emphasised the importance of a Europe-wide cybercrime platform. Embracing the principles enshrined in the Budapest Convention, to which all but three EU Member States are a party, the EU instituted EC3 as a specialised cybercrime centre within Europol. Besides its investigative function, EC3 covers a range of strategic activities, including comprehensive analyses of emerging trends, advice to policymakers concerning cybercrime and providing training to law enforcement authorities within and outside the EU. In order to support the judicial processes behind EC3's investigations, the EU can also call on Eurojust; the latter's main role in combating cybercrime is to facilitate legal processes in cross-border investigations.

Another key priority in the EU is fortifying cyberdefence. However, efforts to develop cyberdefence capabilities in the EU appear to be less interactive and somewhat independent from other aims of resilience building and crime reduction. Admittedly, developments have been slower to come about but the Council has adopted a common Cyber Defence Policy Framework. This Framework highlights the importance of addressing capability gaps in Member States (with respect to CSDP) and advancing international collaboration. Various initiatives are in place to create a common crisis response platform, with an emphasis on developing technical capabilities in detection, response and recovery.

4 CYBERSECURITY CAPABILITIES IN THE UNITED STATES

KEY FINDINGS

- The proliferation of documents, initiatives and agencies within the area of cybersecurity in the United States creates a complex capability landscape, potentially undermining the effectiveness of the response.
- The Department of Homeland Security (DHS) prioritises resilience building in the cyber domain, particularly with respect to securing federal civilian government networks, protecting critical infrastructure and responding to cyberthreats.
- While no single federal agency is tasked with combating cybercrime, various law enforcement agencies have employed divisions dedicated to that aim.
- The new cyberdefence strategy is marked by its focus on offensive capabilities, as well as the United States' willingness to name adversaries.
- Despite many proposals and amendments to facilitate improved information sharing, passage into law remains difficult due to technical and legal challenges, as well as an absence of stakeholder agreement.

The United States' (US) cybersecurity policy has a lengthy history. For nearly two decades, the federal government has issued various strategies and other initiatives, including directives, related to the cybersecurity policy area. Proposed strategies and policies have sought to address infrastructure, software and human interactions. In 1998 the US government began efforts to address cyberspace-related risks, to critical infrastructure in particular, and to create a coordinating structure within the White House, through Presidential Decision Directive (PDD) 63.[237] PPD 63 laid out the ambitious goal of maintaining the ability to protect critical infrastructure from cybersecurity threats within five years.

Cybersecurity strategy was further developed in 2003 through the National Strategy to Secure Cyberspace, which called for a national policy and guiding principles, especially around vulnerability reduction, security response and security awareness training.[238]

4.1 The question of effectiveness enters the debate

The 2009 the Cyberspace Policy Review (the Review), written by the United States Office of the President, raised the question of effectiveness. The preface of the Review noted that the federal government was not organised in a way that would enable it to address the growing problem of cybersecurity effectively, either at the time or in the future.[239] The main reason for this observation was the distribution of responsibilities across a wide array of federal departments and agencies. The problematic nature of this distribution was enhanced by the existence of overlapping mandates and authorities; there was no department or agency with sufficient decision power to guide actions that could deal with conflicting matters in a consistent way. According to the Review, to

[237] White House. 1998. *Presidential Decision Directive/NSC-63*. As of 12 October 2015: http://fas.org/irp/offdocs/pdd/pdd-63.htm
[238] White House. 2003. *The National Strategy to Secure Cyberspace.* As of 12 October 2015: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
[239] White House. 2009. *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communication Infrastructure*. As of 12 October 2015: https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

derive a holistic vision the US government needed to integrate competing interests and develop a plan to address the cybersecurity issues confronting the country as a whole.[240] US President Obama accepted the recommendations set forth in the Review and selected an Executive Branch Cybersecurity Coordinator who had regular access to the president.[241]

The Review's observation was reiterated in 2013 by the US Government Accountability Office (GAO). The GAO indicated that there was no integrated and overarching strategy that synthesised all existing documents in order to provide a comprehensive plan covering priorities, responsibilities and time frames for completion: 'There is no single document that comprehensively defines the nation's cybersecurity strategy.'[242] The main problem identified by the GAO was the absence of clearly defined roles and responsibilities for the key agencies involved in the area of cybersecurity.

This lack of clearly defined roles and responsibilities provides essential contextual information and illustrates the challenge of mapping accurately cybersecurity capabilities in the US, taking into account potential overlaps between the mandates of the agencies involved. As of April 2015, Dourado & Castillo have identified a total of 62 federal offices that declare a cybersecurity mission.[243] However, referring to their publicly available dataset, it is important to note that this figure includes sub-agencies as well as main agencies, which may lead to duplication. Further, this figure does not include some of the agencies included in this chapter, such as the United States Secret Service (USSS) as well as the Immigration and Customs Enforcement (ICE) Cyber Crime Centre (C3) as part of law enforcement in the area of cybercrime. The analysis presented by Dourado & Castillo confirms the complexity of mapping all departments, agencies and sub-agencies in the area of cybersecurity in the US. Even so, perhaps the most crucial observation they make is that many of the offices they found appear to operate with nearly identical mission statements without a clear distinction between operations.[244] This is a theme that will recur later in this chapter as a challenge to the federal government's approach to cybersecurity.

Challenges also surface at state level, as coordination varies from state to state due to different models of governance as well as diversity in terms of the centres of authority responsible for responding to cybersecurity incidents and emergencies. This leads to different levels of maturity between the states.[245] While state-level cybersecurity extends beyond the scope of this study, this observation is nonetheless important due to its resemblance to the situation in the EU with respect to its Member States and how this influences the overall level of cybersecurity effectiveness.

In order to streamline our analysis, we focus on the core agencies and organisations rather than providing a comprehensive overview of all players. The remainder of this chapter follows the top three strategic priorities for cybersecurity capabilities in the EU

[240] White House 2009.
[241] White House. n.d.-a. 'The Comprehensive National Cybersecurity Initiative.' As of 12 October 2015: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
[242] US GAO. 2013. *A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges*. As of 12 October 2015: http://www.gao.gov/assets/660/652817.pdf
[243] Dourado, Eli & Andrea Castillo. 2015. 'Dozens of Federal Cybersecurity Offices Duplicate Efforts with Poor Coordination.' *Mercatus Center*, April 14. As of 12 October 2015: http://mercatus.org/publication/dozens-federal-cybersecurity-offices-duplicate-efforts-poor-coordination
[244] Dourado & Castillo 2015.
[245] United States House of Representatives. 2013. *Joint hearing before the Subcommittee on Emergency Preparedness, Response, and Communications and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security House of Representatives*. As of 12 October 2015: http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg87116/pdf/CHRG-113hhrg87116.pdf

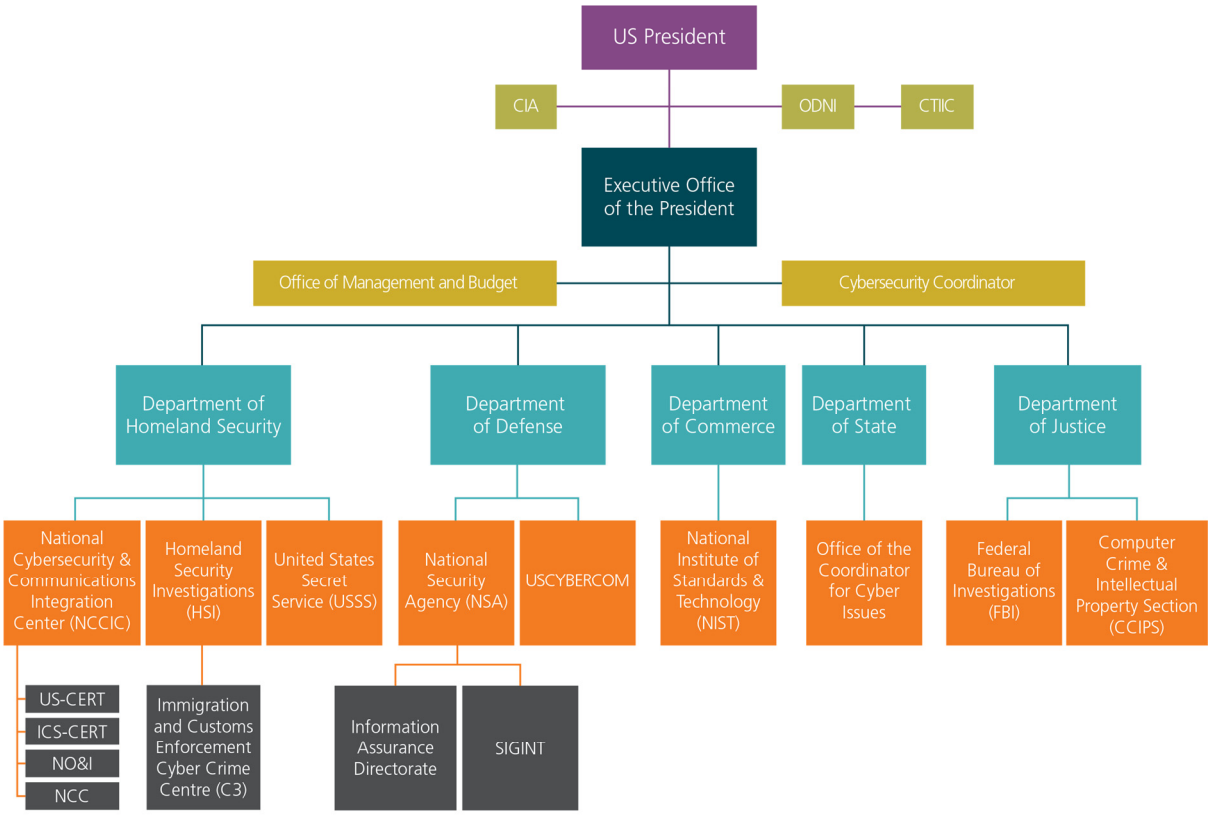
identified in Chapter 3. While US cybersecurity capabilities do not map easily onto the EU strategy framework, we chose this approach because it helps make a more meaningful comparison. The differences between the US and the EU form a caveat to the comparison; for example, a primary focus in the US is on the protection of federal information systems, for which there is no direct equivalent in the EU. Although it is not one of the five strategic priorities, we also provide analysis of US information sharing initiatives, in particular the Cyber Information Sharing Act (CISA), as information sharing permeates all of the strategic priorities and is of increasing priority for the US.

4.2 Brief background on federal government structure

To be able to situate the agencies and departments discussed in this chapter within a context, this section briefly identifies how the US federal government is organised. The government has three branches – legislative, executive and judiciary – and the main focus in this chapter is on 14 departments within the executive branch. These departments are the equivalent of ministries in a parliamentary system. Besides the 14 executive departments, the executive branch also contains the Executive Office of the President. The proliferation of cybersecurity means the topic is included in the activities of a number of departments, including the Department of Homeland Security (DHS), Justice (DoJ) and Defense (DoD), the Department of Commerce and the State Department. Within the Executive Office of the President, the Office of Management and Budget (OMB) is involved in cybersecurity, as is the Cybersecurity Coordinator – a function introduced after the 2009 Review.

Figure 5 provides an overview of the agencies involved within the departments. This list is not meant to be comprehensive, since most departments and their agencies have sub-agencies; this chapter looks at capabilities at a relatively high level of administration.

Figure 5. Overview of US federal government structure



Source: RAND Europe study team

4.3 Achieving cyberresilience

The first strategic priority is the achievement of cyberresilience. This priority falls firmly within the territory of the DHS. The US government established the DHS in the aftermath of the terrorist attacks on 9/11 (2001). The original and primary mission of the DHS focused on preventing terrorist attacks, limiting the nation's vulnerability to them, minimising damage from attacks and increasing US national resilience. Initially, cybersecurity was a 'secondary concern and responsibility'.[246] According to Lowery, the introduction of the Federal Emergency Management Agency (FEMA) led to a wide mission space that paved the way for an 'all-hazards' approach. This does not mean planning for every possible hazard; rather, this identifies commonly occurring hazards that can be addressed by a general, preconceived plan that can be used to tackle unexpected events. Lowery describes the move towards an all-hazards approach as a general trend for the US government since the 1990s. Cybersecurity became a fundamental part of this approach.

Officially, DHS is the leading agency and plays a key role in cybersecurity in the United States. Unofficially, many still see other entities like the National Security Agency (NSA) and US Cybercommand as the true knowledge authorities and leaders in cybersecurity.[247] In 2010, DHS and the DoD signed a memorandum of agreement that put DHS in charge of cybersecurity in the US, with the NSA providing support and expertise.[248] The DHS houses an extensive number of departments and divisions in the area of cybersecurity. According to Jane Holl Lute, DHS is responsible for the following aspects[249]:

- Securing federal civilian government networks[250]
- Protecting critical infrastructure
- Responding to cyberthreats
- Combating cybercrime
- Building partnerships
- Fostering innovation
- Growing and strengthening the cyber workforce.

This list demonstrates how DHS is involved in multiple facets of cybersecurity. In the context of cyberresilience, in this section we focus on the first three responsibilities in this list and reflect briefly on the fourth in Section 4.4 on cybercrime.

---

[246] Lowery, Edward W. 2014. *Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to support the DHS Cyber Security Mission*. Monterey, Calif.: Naval Postgraduate School. As of 12 October 2015: https://www.hsdl.org/?view&did=762425

[247] Sternstein, Aliya. 2015. 'Senators want Homeland Security to be a leading cyber defense agency.' *DefenseOne*, 22 July. As of 12 October 2015: http://www.defenseone.com/technology/2015/07/senators-want-homeland-security-be-leading-cyber-defense-agency/118410; Czech National Security Centre (NCKB). 2015. *National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020*. National Security Authority (NBU). As of 12 October 2015: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_en.pdf, p. 9.

[248] US DHS. 2010. 'Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity.' As of 12 October 2015: http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf

[249] US DHS. 2013a. *Written testimony of DHS Deputy Secretary Jane Holl Lute for a House Committee on Homeland Security hearing titled 'DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure*.' As of 12 October 2015: http://www.dhs.gov/news/2013/03/13/written-testimony-dhs-deputy-secretary-jane-holl-lute-house-committee-homeland

[250] For example, DHS has the lead in protecting the '.gov' and '.com' domains, while the US Cybercommand has the lead in protecting the '.mil' domain.

4.3.1 Securing federal civilian government networks

With respect to securing federal civilian government networks, DHS has operational capabilities to carry out the task of securing unclassified federal civilian government networks (in the '.com' and '.gov' domains). DHS simultaneously and directly supports federal civilian departments and agencies to develop capabilities to improve their cybersecurity stance, especially as a means to comply with the requirements set out by the Federal Information Security Act (FISMA). DHS' lack of formal enforcement power has been a point of contention, in view of the state of (in)security at federal agencies. As Fleming & Goldstein from the Homeland Security Studies and Analysis Institute (HSSAI) write, 'While DHS "has the lead" for the federal government to secure civilian government computer systems, it appears to have no formal enforcement authority to compel federal government departments and agencies to apply recommended cybersecurity mitigations.'[251] In 2015, a group of bipartisan senators introduced the FISMA Reform Act with the objective of formalising the role of DHS in the protection of government networks and websites.[252] According to Collins, the lead Republican senator on the bill, 'While the Department of Homeland Security has the mandate to protect the .gov domain, it has only limited authority to do so.'[253] The proposed FISMA Reform Act would reduce barriers currently in place that prevent DHS from inspecting networks of other agencies. In the current situation, DHS needs permission for the investigation and monitoring of other agencies' networks. The voluntary nature of compliance with FISMA is, according to some involved, part of the problem. To what extent the nature of compliance with FISMA is voluntary appears unclear, since Jeh Johnson noted that, as Secretary of Homeland Security, he had the authority to 'issue Binding Operational Directives to federal departments and agencies'.[254] Johnson went on to explain that 'a Binding Operational Directive is a direction to agencies to mitigate a risk to their information systems', and that after issuing his first Binding Operational Directive on 21 May, 2014, 'departments and agencies responded quickly, and have already reduced critical vulnerabilities covered by the Binding Operational Directive by more than 60 per cent'.[255]

Even so, the general impression remains – at least as communicated through the media, supported by statements from politicians – that DHS lacks the enforcement power to ensure federal agencies and departments implement the necessary security measures to enhance cyberresilience.

Enforcement power, however, is not the only consideration; individual departments and agencies must also implement (basic) security measures. On 4 June, 2015, the US Office of Personnel Management (OPM) issued a press release describing how it had identified a cybersecurity incident that potentially affected data from current and former employees, including personal identifying information (PII).[256] The 4 June press release was only the

[251] Fleming, Matthew H. & Eric Goldstein. 2012. *An analysis of the primary authorities governing and supporting the efforts of the department of homeland security to secure the cyberspace of the United States.* As of 12 October 2015: http://ssrn.com/abstract=2182675
[252] Bennett, Cory. 2015. 'Senators unveil new Homeland Security cyber bill.' *The Hill*, July 22. As of 12 October 2015: http://thehill.com/policy/cybersecurity/248775-senators-set-to-unveil-new-dhs-cyber-bill
[253] Bennett 2015.
[254] US DHS. 2015a. *Written testimony of DHS Secretary Jeh Johnson for a House Committee on the Judiciary hearing titled 'Oversight of the U.S. Department of Homeland Security*.' As of 12 October 2015: http://www.dhs.gov/news/2015/07/14/written-testimony-dhs-secretary-johnson-house-committee-judiciary-hearing-titled-
[255] US DHS 2015a.
[256] United States Office of Personnel Management. 2015. 'OPM to Notify Employees of Cybersecurity Incident.' *Press Release*, June 4. As of 12 October 2015: https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/

beginning of a significant story that, according to the most recent accounts, affected 21.5 million individuals, far more than the 4 million originally identified. At the time of writing, the breach remains a top news story, especially in the US. The data compromised during the breach contained background investigation records of current, former and prospective federal employees and contractors. Due to the sensitivity of the data, many questions have been raised about the security of the federal government's information systems in general and OPM specifically.

After the OPM hack, the White House announced efforts to strengthen and enhance federal cybersecurity. The OMB issued a 30-day cybersecurity sprint in which it identified four action points to improve the state of security and resilience of federal systems.[257] One of those action points was to patch security vulnerabilities as soon as possible. This is a crucial focus, especially considering that, according to research carried out by Veracode, government clients rank last with respect to patching vulnerabilities.[258] Agencies must report to both OMB and DHS with respect to progress and challenges.

The involvement of the OMB after the OPM breach is significant; the OMB has delegated responsibility for improving the cybersecurity of federal civilian agencies to DHS.[259] The GAO was critical of this transfer: 'Although federal law assigns the Office of Management and Budget (OMB) responsibility for oversight of federal government information security, OMB recently transferred several of these responsibilities to DHS […]. It remains unclear how OMB and DHS are to share oversight of individual departments and agencies. Additional legislation could clarify these responsibilities.'[260] In its *Memorandum on Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the DHS*, OMB, along with the Cyber Coordinator, state the following with respect to the responsibility of OMB:

> *OMB will be responsible for the submission of the annual FISMA report to Congress, for the development and approval of the cybersecurity portions of the President's Budget, for the traditional OMB budgetary and fiscal oversight of the agencies' use of funds, and for coordination with the Cybersecurity Coordinator on all policy issues related to the prior three responsibilities*.[261]

With respect to DHS and its responsibility, the memorandum states:

> *DHS will exercise primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543. In carrying out this responsibility and the accompanying activities, DHS shall be subject to general OMB oversight*.[262]

The OMB's initiation of the cybersprint appears – from the outside looking in – to be a result of the oversight exercised over DHS, since the identification of specific action points appears to fall more logically under the responsibility of DHS, based on the above.

---

[257] White House. 2015a. 'Fact sheet: Enhancing and Strengthening the Federal Government's Cybersecurity.' *Office of Management and Budget*, June 12. As of 12 October 2015: https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf

[258] Hesseldahl, Arik. 2015. 'Why the Federal Government sucks at Cyber Security.' *re/code*, 23 June. As of 10 September: http://recode.net/2015/06/23/why-the-federal-government-sucks-at-cybersecurity/

[259] White House. 2010. 'Memorandum for the Heads of Executive Departments and Agencies.' *Office of Management and Budget*, July 6. As of 12 October 2015: https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf

[260] US GAO. 2013. *A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges*. As of 12 October 2015: http://www.gao.gov/assets/660/652817.pdf

[261] White House 2010.

[262] White House 2010.

The Cybersecurity Coordinator – another existing function within the Executive Office of the President as a result of the Review – 'will have visibility into DHS efforts to ensure Federal agency compliance with FISMA and will serve as the principal White House official to coordinate interagency cooperation with DHS cybersecurity efforts'.[263]

Within the US context, the significant emphasis on the protection of federal information systems has been an ongoing theme. The state of security of such information systems has come under increased scrutiny following various incidents, leading to questions about its effectiveness. In addition to the most recent cybersprint initiated by OMB, the National Institute of Standards and Technology (NIST) has also introduced documentation to assist federal agencies in their information security practices.[264] Despite these efforts, implementation appears to remain a challenge. In February 2015, the GAO wrote in a report:

> *Until the White House and executive branch agencies implement the hundreds of recommendations that we and agency inspectors-general have made to address cyber challenges, resolve identified deficiencies, and fully implement effective security programs and privacy practices, a broad array of federal assets and operations may remain at risk of fraud, misuse, and disruption, and the nation's most critical federal and private sector infrastructure systems will remain at increased risk of attack from adversaries*.[265]

Implementation, however, is certainly not trivial or obvious, and as a result must receive close attention.

4.3.2 Protecting critical infrastructure

Homeland Security Presidential Directive 7 assigns responsibility for coordinating all national initiatives for critical infrastructure protection, including cybercomponents, to the DHS. Protecting critical infrastructure is a focal point of cybersecurity in the US. In February 2013 President Obama signed into law Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity*.[266] At the same time, he released Presidential Policy Directive (PPD)-21: *Critical Infrastructure Security and Resilience*. Both initiatives aim to increase the overall resilience of critical US infrastructure.

One of the main components of the EO is the development of a Cybersecurity Framework (the Framework) by the NIST to help critical infrastructure owners and providers to reduce and manage their cyberrisk. Through the Framework, the EO emphasises the need to align policy with regard to critical infrastructure protection. The Framework is to provide a consistent set of standards, methodologies, procedures and processes that govern cyberrisk management.

Underlying this initiative is the recognition that there must be greater 'volume, timeliness, and quality of cyberthreat information shared with US private sector entities'.[267] Without the proactive circulation of information, owners and operators of

---

[263] White House 2010.
[264] National Institute of Standards and Technology (NIST). 2010. *Guide for Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*. NIST Special Publication 800-53A. As of 12 October 2015: http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf
[265] US GAO. 2015. *High Risk Series: An Update*. As of 12 October 2015: http://www.gao.gov/assets/670/668415.pdf
[266] White House. 2013a. 'Executive Order – Improving Critical Infrastructure Cybersecurity.' *Office of the Press Secretary*, February 12 As of 12 October 2015: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[267] White House 2013a.

critical infrastructure cannot identify, assess or manage cyberrisks. The EO recommends a *voluntary* approach to this: 'The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible.' This is further evidenced by the introduction of two initiatives. The first is a voluntary information-sharing platform through which classified cyberthreat information will be shared with eligible critical infrastructure companies and their security service providers. The second is a DHS-led initiative called the Critical Infrastructure Cyber Community (C³ or C Cubed) Voluntary Program, to which interested entities can subscribe for further guidance on the adoption of the Framework. The C³ Voluntary Program aims to: 1) support industry in increasing its cyberresilience; 2) increase awareness and use of the Framework; and 3) encourage organisations to manage cybersecurity as part of an all-hazards approach to enterprise risk management.[268]

The Framework has a notable risk-based approach. The EO requires the identification of critical infrastructure at greatest risk, which would enable prioritised actions by the government as well as independent regulatory agencies. The scope of this identification, however, excludes 'commercial information technology products or consumer information technology services'.[269]

4.3.3 Response to cyberthreats

Response to cyberthreats also falls within the remit of the DHS. Within DHS, the Office of Cybersecurity and Communications (CS&C) is primarily responsible for enhancing the security, resilience and reliability of the nation's cyber and communications infrastructure. The operational arm of the CS&S is the National Cybersecurity and Communications Integration Center (NCCIC). NCCIC coordinates national efforts and works directly with partners across different levels of government.[270] Overall its mission is to lead 'national efforts to analyse threats to critical cyber and communications infrastructure, develop shared situational awareness across a broad set of partners and constituents, and lead the national response to cybersecurity and communications incidents'. NCCIC has been labelled the 'nerve center of the government's civilian cyber and information-sharing operation'.[271] Figure 6 describes the four branches of NCCIC.[272]

[268] US DHS. 2015b. 'About the Critical Infrastructure Cyber Community C3 Voluntary Program.' As of 12 October 2015: http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program
[269] White House 2013a.
[270] US DHS. 2013b. 'DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers.' As of 12 October 2015: https://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-02_Oct13.pdf
[271] Corrin, Amber. 2012. 'DHS feels growing pains in cybersecurity role.' *FCW*, October 17. As of 12 October 2015: http://fcw.com/articles/2012/10/17/dhs-cybersecurity.aspx
[272] US DHS 2013b.

Figure 6. NCCIC branches

Source: RAND Europe study team

Within its operations NCCIC maintains regular, dedicated liaison with 13 US departments and agencies and 16 private sector entities. In addition, NCCIC collaborates and shares information with over 100 private sector entities on a regular basis.[273]

The Office of the Inspector General (OIG) notes how DHS could improve sharing information among the federal centres that coordinate cybersecurity-related activities.[274] Particular challenges identified by the OIG include the observation that NCCIC and federal cybersecurity centres do not all have the same technology and resources, which prevents them from being able to have the same situational awareness of breaches, intrusions and other threats. This leads to coordination challenges in the area of response. The OIG also notes that the centres have not established a standard set of categories for incident reporting.[275]

4.3.4 EINSTEIN: a cyberresilience tool

One specific aspect of DHS's cyberresilience approach is the EINSTEIN system.[276] This system, currently on its third revision, is an early warning, detection and prevention system for intrusions to federal executive branch civilian networks. EINSTEIN aims to provide near real-time identification and automated disruption of malicious activity.

The first iteration of EINSTEIN was developed in 2004 and automated the collection and analysis of computer network security information from participating agencies and government networks. The intention was to help analysts identify and combat malicious

[273] US DHS 2015a.
[274] US DHS 2013b.
[275] US DHS 2013b.
[276] US DHS. 2013c. 'DHS/NPPD/PIA-001 The Einstein Program.' As of 12 October 2015: http://www.dhs.gov/publication/dhsnppdpia-001the-einstein-program

cyberactivity that might threaten government network systems, data protection and communications infrastructure. Five years later, the US government introduced the second iteration of EINSTEIN, which incorporated intrusion detection capabilities into the original system. The third iteration, EINSTEIN 3A (where 'A' stands for 'accelerated') works with DHS's Continuous Diagnostics and Mitigation (CDM) programme. Together, these systems detect and prevent attacks or other suspicious activity from entering federal networks (EINSTEIN 3A) and identify, alert and manage reports of possible attacks inside US government networks (CDM).[277] Deployment of EINSTEIN 3 across government department and agencies was originally scheduled for 2018 but as a result of the OPM breach this has been brought forward to 2016.[278]

4.4 Reducing cybercrime

No agency has been designated as the lead investigative agency in the US for combating cybercrime.[279] Instead various federal law enforcement agencies are involved, many under the DHS. The sheer number of different agencies is due to the fact that, after the establishment of DHS, 22 agencies were realigned under the newly formed department.

4.4.1 United States Secret Service

One of these agencies was the United States Secret Service (USSS).[280] The United States Congress established the USSS investigative powers 30 years ago with the creation of the Computer Fraud and Abuse Act (CFAA)[281] as part of enacting the Comprehensive Crime Control Act of 1984 (P.L. 98-473). Through that law, Congress provided the USSS with the authority to investigate criminal offences related to unauthorised access to computers and the fraudulent use, or trafficking of, access devices – defined as any piece of information or tangible item that is a means of account access and can be used to obtain money, goods, services or other valuable attributes.[282] In his congressional testimony, William Noonan describes how the USSS engages in proactive investigation with respect to cybercrime through a variety of means to infiltrate transnational cybercrime groups. These proactive investigations mean the USSS is often the first to discover an ongoing breach or plans for a breach. This allows the agency to notify quickly the potential victims involved, such as financial institutions and other organisations. It is also able to provide (potential) victims with 'actionable' information to mitigate the damage from a breach and terminate a perpetrator's unauthorised access to the victim's networks. Noonan specifically states:

> *One of the most poorly understood facts regarding data breaches is that it is rarely the victim company that first discovers the criminal's unauthorised access to their network; rather it is law enforcement, financial institutions, or other third*

[277] US DHS. 2015c. 'Einstein 3 Accelerated.' As of 12 October 2015: http://www.dhs.gov/publication/einstein-3-accelerated
[278] Corrin, Amber. 2015. 'Does cyber breach illuminate a $3B DHS failure?' *C4ISR & Networks*, July 13 As of 12 October 2015: http://www.c4isrnet.com/story/military-tech/omr/opm-cyber-report/2015/06/05/opm-breach-einstein-dhs/28556635/
[279] Finklea, Kristin & Theohary, Catherine. 2015. *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. Congressional Research Service, January 15. As of 12 October 2015: https://www.fas.org/sgp/crs/misc/R42547.pdf
[280] Lowery 2014.
[281] Formally 18 U.S.C. §§ 1029 and 1030
[282] US DHS. 2014. *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 titled 'Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future*.' As of 12 October 2015: http://www.dhs.gov/news/2014/05/07/written-testimony-usss-cyber-operations-branch-senate-appropriations-subcommittee

parties that identify and notify the likely victim company of the data breach by identifying the common point of origin of the sensitive data being trafficked in cybercrime marketplaces.[283]

In fact, Verizon's 2014 Data Breach Incident Report (DBIR) found that 70–80 per cent of breaches are reported by unrelated third parties.[284] When the USSS detects an intrusion, the agency contacts the owner of the suspected compromised system. Once the owner confirms the unauthorised access, the USSS works with local US Attorney's Office and other state and local officials, as appropriate, to launch a criminal investigation. The USSS investigates the modus operandi of the unauthorised access and shares this information with the 'widest audience' possible, bearing in mind the integrity of ongoing criminal investigations as well as respecting the privacy and confidentiality of the victim.

To facilitate the inherent transnational nature of cybercrime investigations, the USSS maintains cooperative partnerships with both national and international stakeholders. Noonan identifies the efforts of the Department of State and the Department of Justice International Affairs to carry out Mutual Legal Assistance Treaties (MLATs). The USSS also has agents based at Interpol and Europol.

The statutory enforcement power of the USSS often appears to be neglected or at least not taken into consideration during discussions about the DHS's lack of enforcement power. Lowery highlights several instances during the last few years when the official enforcement power of the USSS has been ignored. He mentions, for example, how DHS launched the website 'Preventing and Defending against Cyber Attacks' to publicise its efforts without making any mention of its law enforcement component.[285] As Lowery describes, before the events of 9/11, the USSS was aligned with the US Department of Treasury, where its expertise and consistent success in financial and cyber investigations received wide recognition.

4.4.2 Immigration and Customs Enforcement – Cyber Crimes Center

The USSS is not the only agency involved in cybercrime. It maintains a close working relationship with another cybercrime wing of DHS, the Immigration and Customs Enforcement (ICE) Cyber Crimes Center, or C3. The origin of C3 dates back to 1997 when the US Customs Service introduced it as a means to respond to developing technologies and their impact on crime. 'C3 delivers computer and cyber-based technical services in support of HSI cases – including investigations into underground online marketplaces selling illegal drugs, weapons and other contraband; the trading of images of child pornography; and the theft of intellectual property.'[286] DHS recently unveiled a major expansion of C3. According to the DHS press release, 'The expanded center will provide ICE's Homeland Security Investigations (HSI) with enhanced operational and training capabilities in order to meet the growing cyber mission of the agency and increasing workload of criminal cases with a cyber-nexus.'[287]

[283] US DHS 2014.
[284] Verizon 2014.
[285] Lowery 2014.
[286] US DHS. 2015d.'DHS Unveils Major Expansion of Ice Cyber Crimes Center.' As of 12 October 2015: http://www.dhs.gov/news/2015/07/22/dhs-unveils-major-expansion-ice-cyber-crimes-center
[287] US DHS 2015d.

4.4.3 Federal Bureau of Investigation

Besides the USSS and ICE C3, the Federal Bureau of Investigation (FBI) also maintains a primary role in combating cybercrime. The USSS and the FBI share jurisdiction for investigations of violations of the Computer Fraud and Abuse Act with regard to cyberintrusions into protected systems.[288] The FBI has a unique dual-role responsibility with regard to cybercrime. The first is its role as the nation's domestic intelligence agency, with responsibility for preventing harm to national security. The second is its role as the nation's principal law enforcement agency, with responsibility for enforcing federal laws.[289] The FBI introduced its dedicated Cyber Division in 2002, according to Lowery to integrate its national security and cyberinvestigative missions.[290] The FBI, in particular the Executive Assistant Director for Criminal, Cyber Response and Services Branch, is responsible for all criminal and cyber investigations worldwide, as well as international operations, critical incident response and victim assistance. The FBI also houses an Internet Complaint Center (IC3), whose mission it is to 'receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cybercrime. The IC3 gives the victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities to suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local, and international level, the IC3 provides a central referral mechanism for complaints involving Internet-related crimes.'[291]

4.4.4 Department of Justice – Computer Crime and Intellectual Property Section

Besides the FBI, the DoJ maintains a Computer Crime and Intellectual Property Section (CCIPS). CCIPS exists to prevent, investigate and prosecute computer crimes by working with other government agencies, the private sector, academic institutions and foreign counterparts. Attorneys within CCIPS aim to improve the domestic and international infrastructure on the legal, technological and operational level to pursue cybercrime perpetrators most effectively. Besides computer crime, CCIPS also maintains responsibilities in the area of intellectual property crimes, which are similarly 'multi-faceted'. To carry out these objectives:

> *CCIPS attorneys regularly run complex investigations, resolve unique legal and investigative issues raised by emerging computer and telecommunications technologies; litigate cases; provide litigation support to other prosecutors; train federal, state, and local law enforcement personnel; comment on and propose legislation; and initiate and participate in international efforts to combat computer and intellectual property crime*.[292]

4.4.5 The National Cyber Investigative Joint Task Force (NCIJTF)

The FBI leads the National Cyber Investigative Joint Task Force (NCIJTF), which 'serves by Presidential Directive as the national focal point for coordinating cyberthreat

---

[288] Doyle, Charles. 2014. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Stature and Related Federal Criminal Laws.* Congressional Research Service, October 15. As of 12 October 2015: https://www.fas.org/sgp/crs/misc/97-1025.pdf

[289] FBI. n.d. 'Addressing Threats to the Nation's Cybersecurity.' As of 12 October 2015: https://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1

[290] Lowery 2014.

[291] Internet Crime Complaint Center (IC3). n.d. 'About Us.' As of 12 October 2015: https://www.ic3.gov/about/default.aspx

[292] US DoJ. n.d. 'Computer Crime and Intellectual Property Section (CCIPS).' As of 12 October 2015: http://www.justice.gov/criminal-ccips

investigations'. [293] Representatives from the US Intelligence Community (IC) member agencies, as well as select federal law enforcement partners, are present in the task force and collaborate in identifying, mitigating and disrupting cybersecurity threats. Quinn states that 19 US agencies and Five Eyes (FVEY) partners are able to coordinate cyberthreat investigations at an unprecedented level at the NCIJTF.[294] Besides the FBI, as its leader, the NCIJTF contains deputy directors from the NSA, DHS, the Central Intelligence Agency (CIA), the USSS and the US Cyber Command. Throughout 2013 and 2014, partners from FVEY[295] joined the existing group of officials through liaison officers. By creating these partnerships, NCIJTF 'is working to become the international leader in synchronizing and maximizing investigations of cyber adversaries'.[296]

4.5 Fortifying cyberdefence

The Department of Defense (DoD) is at the forefront of improving cyberdefence in the United States. Over the last few years, several strategies have been published that provide high-level insight into the role of the DoD in the development of cyberdefence policy. The DoD has three primary cyber missions:

- Defend DoD networks, systems, and information.
- Defend the US homeland and US national interests against cyberattacks of significant consequence.
- Provide cyber support to military operational and contingency plans.

The US Secretary of Defense directed the Commander of the US Strategic Command to establish a sub-unified command, United States Cyber Command (USCYBERCOM), in June 2009, with full operational capability achieved in October 2010.[297]

In July 2011, the DoD published its *Department of Defense Strategy for Operating in Cyber Space*.[298] Lawson relates how the strategy received considerable criticism, for being 'too defensive' and 'for not being a strategy at all'.[299] Moreover, he indicates how, despite the claim that the 2011 strategy was introduced as the first DoD strategy for cyberspace, other documents preceded it. The National Military Strategy for Cyberspace Operations (NMS-CO) came out in 2006 and instructs the DoD 'to be prepared to support DHS, as the lead USG agency'.[300] The NMS-CO, however, also acknowledges:

> *If defense of a national interest is required, DoD's national defense missions, when authorized by Presidential orders or standing authorities, take primacy*

[293] FBI. n.d.
[294] Quinn, Richard. 2014. 'Statement before the House Homeland Security Committee, Subcommittee on Cyber Security, Infrastructure Protection, and Security Technologies.' *FBI Testimony*, April 16. As of 12 October 2015: https://www.fbi.gov/news/testimony/the-fbis-role-in-cyber-security
[295] United Kingdom, United States, Canada, Australia and New Zealand.
[296] Quinn 2014.
[297] US Strategic Command. 2015. 'US Cyber Command.' As of 12 October 2015: https://www.stratcom.mil/factsheets/2/Cyber_Command/
[298] United States Department of Defense (US DoD). 2011. *Department of Defense Strategy for Operating in Cyberspace*. As of 12 October 2015: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf
[299] Lawson, Sean. 2011. 'DOD's "First" Cyber Strategy is Neither First, Nor a Strategy.' *Forbes,* August 1. As of 12 October 2015: http://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/
[300] United States Joint Chiefs of Staff. 2013. *Cyberspace Operations*. Joint Publication 3-12(R), 5 February. As of 12 October 2015: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

> *over, and many subsume, the standing missions of other departments and agencies*.[301]

According to Lawson, the connection between the two documents is unclear. In the same year as the published DoD strategy, the GAO issued a report indicating its perspective on the manner in which DoD handled cyberrelated activities. According to the GAO:

> *Several joint doctrine publications address aspects of cyberspace operations, but DoD officials acknowledge that the discussions are insufficient; and no single joint publication completely addresses cyberspace operations. While at least 16 DoD joint publications discuss cyberspace-related topics and 8 mention 'cyberspace operations,' none contained a sufficient discussion of cyberspace operations*.[302]

This conclusion appears comparable to the one drawn by the GAO in the civilian space. In connection with the DoD, the GAO noted more specifically in 2011 that 'conflicting guidance and unclear responsibilities have created challenges for command and control of cyberspace operations'.[303]

An oft-cited case was a computer infection that spread via a USB stick in 2008 and allowed perpetrators to gain access to classified networks. This incident was hampered by a lack of operational clarity[304] and led to a massive revamping of cybersecurity requirements and implementation of new defensive measures. The clean-up and subsequent defensive actions were named 'Operation Buckshot Yankee'. As part of the National Defense Authorization Act (NDAA) of 2014, the US Congress required the DoD to designate a Principal Cyber Advisor to the Secretary of Defense 'to review military cyberspace activities, cyber mission forces, and offensive and defensive cyber operations and missions. In addition, the Principal Cyber Advisor will govern the development of DoD cyberspace policy and strategy for the DoD enterprise.'[305] Moreover: 'The 2014 NDAA also stipulated that this Principal Cyber Advisor integrate the cyber expertise and perspectives of key organizations to build an intradepartmental team of key players to ensure effective governance of cyber issues within DoD.'[306]

4.5.1 Revised cybersecurity strategy

In April 2015, the DoD published a new cybersecurity strategy.[307] The DoD recognised three drivers that led to its introduction. First, the DoD described how the severity and sophistication of cyberthreats to US interests, including DoD networks, is increasing. As a result, the DoD felt compelled to introduce more aggressive measures to counter such threats. The second driver was the request issued by President Obama in 2012 for the DoD to organise and plan a defence for the US against cyberattacks with significant consequences and for this plan to be in congruence with other US government agencies. The DoD notes how 'this new mission required new strategic thinking'. The third driver was the provision of clear guidance on the development of the US military's Cyber Mission Force (CMF). The DoD started building the CMF in 2012 in response to the enhanced perceived threat. The ultimate goal is for the CMF to 'include nearly 6,200

[301] United States Joint Chief of Staff 2013.
[302] US GAO. 2011. *Defense Department Cyber Efforts: DoD Faces Challenges in its Cyber Activities*. As of 12 October 2015: http://www.gao.gov/assets/330/321818.pdf
[303] US GAO 2011.
[304] US GAO 2011.
[305] US DoD. 2015a. *The DoD Cyber Strategy*. As of 12 October 2015: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
[306] US DoD 2015a, p. 29.
[307] US DoD 2015a.

military, civilian, and contractor support personnel from across the military departments and defence components'.[308] The CMF is composed of forces to 1) defend the US against strategic attack; 2) operate and defend the DoD information networks (DODIN); and 3) provide combatant command support.[309]

On a general note, the main difference between the previous strategy and the latest one is that the US has become more explicit about its capabilities and naming adversaries.[310] For example, in its most recent cybersecurity strategy, the US specifically mentions China in connection with intellectual property theft. The Strategy also mentions Russia, Iran, and North Korea as adversaries in the cyberspace domain. However, the DoD also notes the blend of actors and difficulty of attribution: 'State and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation."[311] Since attribution is such a challenging yet essential feature of cyberspace operations, the DoD has invested significantly in all its source collection, analysis and dissemination capabilities. It has done this with the intention of reducing the anonymity of both state and non-state actors. It notes: 'Intelligence and attribution capabilities help to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics, techniques, and procedures. Attribution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack.'[312]

According to Farrell, based on the latest strategy, the US is no longer worried about a 'cyber Pearl Harbor'.[313] He also observes that the US is increasingly open about its development of its defensive and offensive capabilities. While the government was reserved about admitting such capabilities in the past, the strategy now states that 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'.[314] Deterrence is also a crucial part of the Strategy.[315] This was emphasised by experts prior to its publication[316] but deemed to be very difficult for cyberspace, especially due to the continuing challenge of attribution.

The DoD refers to its role in the area of cyberresilience but also identifies the boundaries of that role. It states specifically that it cannot 'foster resilience in organizations that fall outside of its authority'. As a result, for resilience to function as a successful factor in effective deterrence, other government agencies must cooperate with critical

[308] US DoD.2015b. 'Fact Sheet: Department of Defense Cyber Strategy.' As of 12 October 2015: http://www.defense.gov/home/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf
[309] United States Air Force. n.d. 'USCYBERCOMMAND Cyber Mission Force.' Headquarters US AirForce, Power Point Presentation. As of 12 October 2015: http://www.safcioa6.af.mil/shared/media/document/AFD-140512-039.pdf
[310] Sanger, David. 2015. 'Pentagon Announces New Strategy for Cyberwarfare.' *The New York Times*, April 24. As of 12 October 2015: http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html
[311] US DoD 2015a, p. 9.
[312] US DoD 2015a, p. 9.
[313] Farrell, Henry. 2015. 'What's New in the U.S. Cyber Strategy.' *The Washington Post,* April 24. As of 12 October 2015: http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/04/24/whats-new-in-the-u-s-cyber-strategy/
[314] US DoD 2015a.
[315] US DoD 2015b.
[316] Sukhovey, Darya & Miroshnichenko, Olga. 2014. 'American Political Experts on Cyber Security.' *World Applied Sciences Journal* 31(4): 559-561

infrastructure providers within the private sector to develop and maintain resilience and redundancy[317] in a broader way to withstand attacks.[318]

4.6 Information sharing

One particularly advanced area of US policy on cybersecurity is information sharing. Discussion of this can inform the EU as it seeks to consolidate its own approach to cybersecurity generally and information sharing more specifically. This is a more general focus of national security efforts, especially post-9/11, to consolidate (cyber) threat information from various federal departments, supporting state and local agencies and private entities. However, the origins of the call for more information sharing can be traced back even further. As Libicki testifies, 'People have been calling for greater information-sharing for almost 20 years, dating back to the formation of Information Sharing and Analysis Centers (ISACs) in the late 1990s and continuing through the recent reformulation of ISACs into Information Sharing and Analysis Organizations (ISAOs).'[319] Jackson describes how the policy debate on information sharing contains strong views from directly affected stakeholders, such as private companies, but weak data. Information sharing can be a polarising issue of public policy. Jackson states:

> *Reflecting the interest in information sharing as a component of domestic security since 9/11, the policy literature is replete with analyses that argue the need for 'more' information sharing (over an undefined current baseline) and analyses arguing that existing efforts are not working to achieve their goal of shared data*.[320]

Zheng & Lewis recognise that information sharing is not a cure-all solution. Yet information sharing is a critical step towards the enhancement of cybersecurity.[321] Zheng & Lewis identify numerous federal efforts made to promote information sharing, in particular between organisations in the private and the public sector.[322]

Besides these more formal efforts, other developments in the area of information sharing have also taken place, in a more organic manner. The primary illustration of this development is the introduction of information-sharing analysis centres, or ISACs. ISACs are an international phenomenon and are generally organised along critical infrastructure sectors, such as finance, energy and aviation. Zheng & Lewis also acknowledge how certain efforts or partnerships introduced to advance information sharing have proven

---

[317] In engineering, redundancy refers to the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or failsafe.
[318] US DoD. 2015a, p. 11.
[319] Libicki, Martin C. 2015. *Sharing Information about Threats is not a Cybersecurity Panacea*. Santa Monica, Calif.: RAND Corporation. CT-425. As of 12 October 2015: http://docs.house.gov/meetings/HM/HM08/20150304/103055/HHRG-114-HM08-Wstate-LibickiM-20150304.pdf
[320] Jackson, Brian. 2014. *How Do We Know What Information Sharing Is Really Worth?* Santa Monica, Calif.: RAND Corporation. As of 12 October 2015: http://www.rand.org/pubs/research_reports/RR380.html
[321] Zheng, Denise & James Lewis. 2015. *Cyber Threat Information Sharing - Recommendations for Congress and the Administration.* Centre for Strategic & International Studies (CSIS). As of 12 October 2015: http://csis.org/files/publication/150310_cyberthreatinfosharing.pdf
[322] These include:

- The Department of Homeland Security's (DHS) Cyber Information Sharing and Collaboration Program (CISCP).
- The Federal Bureau of Investigation's (FBI) Infraguard, which shares cyberthreat information with a broad community of industry stakeholders.
- The Defense Industrial Base Cyber Pilot, which merged with DHS's Enhanced Cybersecurity Services (ECS) program in 2013.
- The Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP).

ineffective, due, for example, to programmatic, technical or legal challenges, as well as an absence of stakeholder commitment. With respect to the US Congress, members of both the US House of Representatives and the US Senate have introduced a number of bills focusing on the enhancement of information sharing in the area of cybersecurity. None of these efforts, according to Zheng & Lewis, has been able to advance into law primarily due to concerns related to privacy and law enforcement use of shared information. Other challenges have focused on the role of the government in information-sharing mechanisms; the lack of reciprocity for the private sector has been an obstacle to generating sufficient support.

4.6.1 Proposed legislation and initiatives

Fischer & Logan provide an overview of cybersecurity and information-sharing initiatives through a comparison of US House of Representatives and US Senate bills introduced in the 114th Congress (3 January 2015–3 January 2017). A total of five bills have been introduced so far in 2015. These are:

- H.R. 1560, the Protecting Cyber Networks Act (PCNA).
- H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 (NCPAA).
- S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA), which was proposed as an amendment to H.R. 1735, the National Defense Authorization Act (NDAA).

Fischer & Logan describe how PCNA, NCPAA and CISA share a number of similarities but also notable differences: 'All focus on information sharing among private entities and between them and the federal government. [If they become laws,] NCPAA would explicitly amend portions of the Homeland Security Act of 2002, and PCNA would amend parts of the National Security Act of 1947. CISA addresses the roles of the Department of Homeland Security and the intelligence community but does not explicitly amend either act.'[323] Relevant provisions have also appeared in other bills. Moreover, the White House has submitted a legislative proposal on the topic in addition to an Executive Order.

4.6.1.1 Cybersecurity Information Sharing Act

The LIBE committee of the European Parliament expressed specific interest in the Cybersecurity Information Sharing Act (CISA S.2588, 113th Congress; CISA S.754, 114th Congress). CISA is a legislative proposal and its primary goal is to 'improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes'. More specifically, the bill 'requires the Director of National Intelligence (DNI), the Secretary of Homeland Security (DHS), the Secretary of Defense (DOD), and the Attorney General (DOJ) to develop and promulgate procedures for classified and declassified cyberthreat indicators' to be shared in real time by the federal government with all relevant entities in the private sector, as well as non-federal, state, tribal and local governments.[324] The bill has received significant criticism from consumer and privacy advocacy groups such as the Electronic Frontier Foundation

[323] Fischer Eric A. & Stephanie M. Logan. 2015. *Cybersecurity and information sharing: Comparison of House and Senate bills in the 114th Congress.* Congressional Research Service, August 5. As of 12 October 2015: https://www.fas.org/sgp/crs/misc/R44069.pdf
[324] United States Congress. 2014. *S.2588 - Cybersecurity Information Sharing Act of 2014*. As of 12 October 2015: https://www.congress.gov/bill/113th-congress/senate-bill/2588

(EFF), Electronic Privacy Information Center (EPIC), American Civil Liberties Union (ACLU) and others. Certain political representatives have also been critical of its potential privacy implications.[325] This resistance has generally been linked to the revelations of Edward Snowden, which have led to challenges about trust with respect to certain federal government agencies that may be recipients of the information, according to the provisions included in the draft CISA.

In the US Senate report, Senator Susan Collins provides additional views on the draft legislation and proposes a two-tier system.[326] The focus of the senator's comments is specifically geared towards the vulnerability introduced through critical infrastructure owners and providers. Senator Collins suggests having a tier that is driven by voluntary information sharing or reporting, which according to the senator would concern 99 per cent of businesses, and a second tier that focuses on the remaining 1 per cent, organisations involved in critical infrastructure sectors, which would be required to engage in mandatory reporting. Certain sectors in the US are already subject to mandatory information sharing. Notable examples include the chemical industry and the electricity, financial and transportation sectors.[327] Even though her amendment has not been adopted, it bears mentioning in the context of the discussion surrounding information-sharing mechanisms, especially in light of comparisons with the EU (see Chapter 6).

4.6.1.2 Executive Order 13691

The focus on owners and providers within critical infrastructure sectors also becomes evident through a White House initiative in the area of information sharing. President Obama signed into law Executive Order (EO) 13691 – Promoting Private Sector Cybersecurity Information Sharing – in February 2015. The EO focuses on encouraging cybersecurity collaboration in the private sector, enabling private-public information sharing and providing strong privacy and civil liberties protection.[328] This includes encouraging the development of information-sharing organisations, like Information Security and Analysis Organisations (ISAOs).[329] The EO also aims to facilitate the development of a common set of voluntary standards for these ISAOs, as well as to clarify DHS's authority to engage in agreements with ISAOs. From a perspective of reciprocity, the EO also aims to simplify private sector organisations' access to classified cybersecurity threat information.

4.6.1.3 Cyber Threat Intelligence Integration Center

In February 2015, President Obama announced the introduction of a Cyber Threat Intelligence Integration Center (CTIIC). The CTIIC will be placed under the auspices of the Director of National Intelligence (DNI). The introduction of CTIIC came about as a result of the current absence of a single government entity responsible for producing

[325] McNeal, Gregory S. 2014. 'Controversial Cybersecurity Bill Known As CISA Advances Out Of Senate Committee.' *Forbes*, July 9. As of 12 October 2015: http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/

[326] Burr, Richard. 2015. *Report together with additional views – Cybersecurity Information Sharing Act 2015*. Congress.gov, 15 April. As of 12 October 2015 : https://www.congress.gov/114/crpt/srpt32/CRPT-114srpt32.pdf

[327] Fischer & Logan 2015.

[328] White House. 2015b. 'Fact Sheet: Executive Order promoting private sector cybersecurity information sharing.' *Office of the Press Secretary*, February 12. https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform

[329] White House 2015b.

coordinated cyberthreat assessments. As Secretary of Homeland Security Jeh Johnson notes, CTIIC is primarily created to 'connect the dots' related to foreign cyberthreats.[330]

Through CTIIC, the US government hopes to ensure that information is shared rapidly among existing Cyber Centers and other governmental entities. It is also anticipated that CTIIC will be able to provide operators and policymakers with timely intelligence about the latest cyberthreats and threat actors.[331] The H.R. 2596 – Intelligence Authorization Act for FY 2016, the bill intended to clarify the creation of CTIIC, came under criticism from the White House. In an official statement, the OMB states, with regard to provisions in the bill relating to the creation of the CTIIC: 'This bill seeks to significantly expand CTIIC's roles and responsibilities beyond those contained in the President's February 25 memorandum directing the establishment of the CTIIC. Further, the bill gives the CTIIC certain intelligence mission management functions already assigned elsewhere.'[332] The OMB goes on to state: 'The limits this bill would place on CTIIC's resources, and the expansive approach the bill would take with regard to CTIIC's missions, are unnecessary and unwise, and would risk the CTIIC being unable to fully perform the core functions assigned to it in the bill.'[333] The problem presented by the bill, according to the OMB, is the intention of expanding the scope of activities and responsibilities of the CTIIC while simultaneously limiting its resources to 50 permanent positions.[334]

4.6.2 Issues in the information-sharing debate

Fischer & Logan identify a number of issues that together comprise the core of the debate on information sharing. They include:

- **Kinds of information**. What kinds of information should be shared but are affected by barriers to sharing that make effective cybersecurity more difficult? What are those barriers?
- **Information-sharing process**. How should the gathering and sharing of information be structured in the public and private sectors to ensure that it is efficient, effective and appropriate?
- **Uses of information**. What limitations should be placed on how shared information is used?
- **Standards and practices**. What improvements to current standards and practices are needed to ensure that information sharing is useful and efficient for protecting information systems, networks and their contents?
- **Privacy and civil liberties**. What are the risks to the privacy rights and civil liberties of individual citizens associated with sharing different kinds of cybersecurity information, and how can those rights and liberties best be protected?

---

[330] US DHS. 2015e. *Remarks by Secretary of Homeland Security Jeh Johnson at the RSA Conference 2015*. As of 12 October 2015: http://www.dhs.gov/news/2015/04/21/remarks-secretary-homeland-security-jeh-johnson-rsa-conference-2015

[331] Tehan, Rita. 2015. *Cybersecurity: Authoritative Reports and Resources, by Topic.* Congressional Research Service, April 28. As of 12 October 2015: https://www.fas.org/sgp/crs/misc/R42507.pdf

[332] White House. 2015c. 'Statement of Administration Policy: H.R. 2596 – Intelligence Authorization Act for FY 2016.' *Office of Management and Budget*, June 15. As of 12 October 2015: https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saphr2596r_20150615.pdf

[333] White House 2015c.

[334] Carman, Ashley. 2015. 'White House criticizes bill clarifying Cyber Threat Intelligence Integration Center missions.' *SC Magazine*, June 22. As of 12 October 2015: http://www.scmagazine.com/obama-administration-issues-statement-on-intelligence/article/422126/

- **Liability protections**. What, if any, statutory protections against liability are needed to reduce disincentives for private-sector entities to share cybersecurity information with each other and with government agencies, and how can the need to reduce such barriers best be balanced against any risks to well-established protections?

Fischer & Logan describe several challenges associated with information sharing in general and to the proposed changes in particular. Perhaps more importantly, however, they emphasise, citing Libicki, that information sharing is merely one facet of cybersecurity and should neither overshadow nor negate the importance of other measures (e.g. patching software, encrypting data, etc.). Fischer & Logan specifically relate this point to the OPM breach and describe how enhanced information sharing would not necessarily have resulted in more effective defence against the attacks, considering the shortcomings in the implementation of FISMA requirements at OPM.[335] Libicki states another reason why information sharing should not be overemphasised: 'Many otherwise serious people assert that information-sharing could have prevented many headline assaults on important networks. Yet, if one works through such attacks to understand if there were precedents that could have given us threat signatures, one often finds no good basis for such a belief. Quelling the nation's cybersecurity problems is a complex, multi-faceted endeavor not subject to a silver bullet.'[336] Libicki explicitly questions whether information sharing deserves the political and public energy it is receiving.

4.7 Overview of US cybercapabilities

Table 6 illustrates the overlaps in the cybersecurity objectives of different US departments and identifies sub-agencies within them.

Table 6. US cybercapabilities with respect to cyberresilience, cybercrime and cyberdefence

US cybercapabilities	Cyberresilience	Cybercrime	Cyberdefence
Department of Homeland Security (DHS)	**Secures** federal civilian government networks (in the .com and .gov domains) **Produces** Vulnerability Scan Reports each week and oversees the progress of agencies in undertaking responses **Protects** critical infrastructure **Responds** to cyberthreats **Builds** partnerships **Strengthens** cyber workforce **Shares** information through numerous platforms ***National Cybersecurity and Communications***	***United States Secret Service (USSS)*** **Investigates** cybercrime such as unauthorised access to computers and the fraudulent use or trafficking of access devices, and shares information through various channels and publications **Oversees** the activities of the Cyber Crimes Center (EC3) of the ICE	

[335] Fischer & Logan 2015.
[336] Libicki 2015.

	Integration Center (NCCIC) **Supervises** four branches: NCCIC Operations and Integration (NO&I), United States Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and National Coordinating Center for Telecommunications (NCC)		
Department of Justice (DOJ)	***Federal Bureau of Investigations (FBI)*** **Oversees** Infraguard, a platform for sharing cyberthreat information with a broad community of industry stakeholders	**Maintains** Computer Crime and Intellectual Property Section which prevents, investigates and prosecutes computer crimes in collaboration with other government agencies, private sector, academic institutions and foreign counterparts ***Federal Bureau of Investigations (FBI)*** **Serves** as the nation's domestic intelligence agency and principal law enforcement agency **Houses** Internet Crime Complaint Center (IC3), which responds to reports filed by victims of cybercrime **Leads** the National Cyber Investigative Joint Task Force (NCIJTF), which seeks to identify, mitigate and disrupt cybersecurity threats with the help of intelligence alliance, Five Eyes (FVEY)	
Department Of Defense (DOD)			**Defends** Department of Defense networks, systems and information **Defends** the US homeland and national interests against cyberattacks of significant consequence **Provides** cyber support to military

		operational and contingency plans **Oversees** the development of US military's Cyber Mission Force (CMF) ***CYBERCOM*** **Directs** the operations and defence of specified Department of Defense information networks **Prepares** to conduct full-spectrum military cyberspace operations **Ensures** US/Allied freedom of action in cyberspace while denying the same to the adversaries

4.8 Conclusion

The US has a lengthy history in the area of cybersecurity. According to one account, 62 federal offices have declared a cybersecurity mission. This relatively large number demonstrates that cybersecurity is a crowded policy implementation space in the US and has led to a number of challenges due to overlapping mandates.

First, the potential overlap between the mandates of DHS and the FBI has been a challenging area. While the relationship between the two entities has, according to the Review Commission, improved greatly during the past 18 months, it remains a work in progress. Due to the broad statutory language that established the responsibility of DHS, there is significant overlap with the FBI's mission space. As the Review Commission puts it: 'The introduction of a new department with a mission to share information with local law enforcement and the private sector, areas where the FBI had developed long-standing relationships in support of its missions, was almost certainly going to result in bureaucratic conflict.'[337] While the relationship between the DHS and FBI has improved in the area of counterterrorism, there has been less progress in the area of cybersecurity. The coordination challenge is largely the result of a lack of clarity about roles and responsibilities at the national level. [338] The GAO arrived at the same conclusion in its analysis. The Review Commission also specifically notes that, while the federal government tries to coordinate the overlapping responsibilities of federal agencies, the private sector remains in the dark. Moreover, the 'muddled national cyber architecture' limits the efforts made in the area of cybersecurity by the FBI and will continue to have consequences for its relationship with DHS. To address this issue, all parties need to be involved.[339]

Second, the official leader in the area of cybersecurity is the DHS but unofficially the NSA and the DoD are perceived as authorities on the topic. The DHS's lack of

[337] Hoffman, Bruce, Edwin Meese & Timothy Roemer. 2015. *The FBI: Protecting the Homeland in the 21st Century*. Report of the Congressionally-directed 9/11 Review Commission. As of 12 October 2015: https://www.fbi.gov/stats-services/publications/protecting-the-homeland-in-the-21st-century, p. 80
[338] Hoffman et al. 2015.
[339] Hoffman et al. 2015.

enforcement abilities has also been a topic of discussion, especially since a number of high-profile intrusions (of which the OPM hack is the most recent and prominent example) have led to questions about the level of security of federal information systems. This incident led to the introduction of the cybersprint initiative by the OMB, which had originally delegated its responsibility for cybersecurity to the DHS. The need for a cybersprint demonstrates the lack of implementation on the part of federal agencies and departments. The GAO has been particularly critical of the lack of attention devoted to its recommendations on improving the cybersecurity stance of various federal agencies and departments. The presence of EINSTEIN 3A (and the CDM programme) ought to improve cyberresilience since they are built to be advanced tools for early warning, detection diagnostics and mitigation. The deployment of the most recent version of EINSTEIN 3A has been brought forward as a result of the OPM breach.

In the area of reducing cybercrime, the US certainly appears to be a leading example. Although no agency has been designated as the lead investigative agency, various federal law enforcement agencies and departments cooperate to reduce cybercrime. These include the FBI, the USSS and ICE C3. Yet again, as with cyberresilience, overlapping mandates lead to challenges. The third strategic objective focused on cyberdefence appears to be a slightly less crowded policy space. The DoD leads cyberdefence initiatives and published a renewed strategy in 2015 in which it elaborates on its plans for the US CMF. The DoD also became more open about its offensive and defensive capabilities as well as its primary state adversaries.[340]

The overarching theme of information sharing further demonstrates the complexity of the cybersecurity landscape in the US. Despite the existence of NCCIC, which shares information with five federal cybersecurity centres, covering the three main objectives of cyberresilience, cybercrime and cyberdefence, information sharing remains a recurring theme of discussion. This is especially apparent in President Obama's authorisation in February 2015 of another centre focused on sharing threat intelligence, CTIIC. While CTIIC aims to fill a void in establishing a comprehensive cyberthreat assessment, introducing a new player to an already crowded policy space is a noteworthy development.

[340] Sanger 2015.

5 TRANSNATIONAL COOPERATION IN THE FIGHT AGAINST CYBERCRIME

KEY FINDINGS

- The EU and the US could develop closer transatlantic law enforcement coordination.
- Public-private partnership is imperative to tackle comprehensively the ever-evolving threat posed by cybercrime.
- Unilateral actions by the different entities illustrate the need for deconfliction; in particular, continuous engagement with the private sector and among law enforcement agencies is needed.
- The Mutual Legal Assistance (MLA) process has been identified as outdated and a hurdle for the effective acquisition of information.
- EU policymakers face the challenge of finding a workable balance between safeguarding personal information and allowing law enforcement agencies to protect the public from cybercriminal activities in an efficient manner.
- Greater harmonisation in policy measures in the EU is required to facilitate the flow of information between the private sector, the police and the prosecution, across and within countries.

5.1 Introduction

The global reach of the Internet defines the cybersecurity threat landscape. The ability to counter cyberthreats, especially emanating from cybercrime, is therefore beyond the scope of any single nation state. Perpetrators carry out cybercrime in various locations as they search for victims around the globe. The need to engage in transnational cooperation to counter the complex challenge posed by cybercrime is widely recognised both inside and outside the European Union (EU).[341] Europol, for instance, notes that, due to the increasing number of cyberthreats emanating from outside the EU, law enforcement agencies must explore strategic and operational cooperation, as well as capacity-building possibilities, with states from which cyber criminals are operating.[342] The European Parliament's own resolution of 12 September 2013, on a Cyber Security Strategy of the European Union, resonates with this assessment by focusing on the importance of intensifying cooperation with other countries to facilitate the exchange of experience and information, complementing activities while avoiding duplication and assisting in the development of cybercapabilities globally to increase cyberresilience and strengthen the fight against cross-border cybercrime locally.[343]

The use of the word 'transnational' as opposed to 'international' is deliberate. Cooperation goes beyond state-to-state partnerships and must involve the private sector. Europol, for instance, is actively seeking out companies by signing strategic

[341] Interview conducted by RAND Europe with the FBI, Europol and the UK National Crime Agency (NCA).
[342] Europol. 2014a. *The Internet Organised Crime Threat Assessment (iOCTA)*. As of 12 October 2015: https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf
[343] European Parliament. 2013a. *Resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. 2013/2606(RSP). As of 12 October 2015: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0376+0+DOC+XML+V0//EN

Memoranda of Understanding, appointing representatives to participate in the European Cyber Crime Centre (EC3) advisory group and reaching out to the academic community through EC3's Academic Advisory Network (EC3AA), to strengthen sectoral cooperation and combine and harness expertise in the fight against cybercrime.[344] In the area of developing mitigation and response strategies in particular, the private sector is becoming an ever more crucial partner to law enforcement agencies as it holds most of the relevant data and potential evidence.[345] Therefore combating cybercrime must take into account the multi-stakeholder nature of the Internet and its governance.

This chapter aims to develop an understanding of how transnational cooperation works in practice from both a strategic and operational perspective, with the intention of illustrating what works well and what challenges remain. The first part of the chapter reflects briefly on strategic cooperation through an overview of the EU-US Working Group on Cybersecurity and Cybercrime (the Working Group). The second part aims to provide a better understanding of transnational cooperation through two case studies that are largely based on publicly available information, for example, press releases issued by agencies such as EC3 and the United States (US) Federal Bureau of Investigation (FBI). The third part focuses on the challenges remain in the area of transnational cooperation in the fight against cybercrime. The basis for the identification of these challenges is interviews with a limited number of individuals active in EU, Member State and non-Member State institutions. These are as far as possible supplemented with additional literature. The fourth part of this chapter focuses on recommendations for improvement gathered through the interviews and concludes with reflections on the state of transnational cooperation.

5.2 Strategic cooperation: EU-US Working Group on Cybersecurity and Cybercrime

The EU and the US face a very similar cyberthreat landscape, although there are some differences in legal regulations and technical standards.[346] Cybercriminals are attracted to European countries and the US by their financial strength, bandwidth consistency and the large number of Internet Service Providers (ISPs).[347] As a result, it has become commonplace, for instance, for banking malware starting in the EU to gravitate to the US or vice versa, or in some cases to infect both simultaneously.[348]

As an example of strategic cooperation, the study team was asked by the European Parliament (EP) to investigate the Working Group, which is the first transatlantic dialogue to tackle these common challenges and offer senior officials an opportunity to foster mutual cooperation on cybersecurity and cybercrime issues.[349] The Working Group was created during the 2010 EU-US Summit in Lisbon to address four key areas:

[344] Europol. n.d.-a. 'Agreements.' As of 2 September, 2015: https://www.europol.europa.eu/category/news-category/agreements; Europol. n.d.-c. 'EC3 Programme Board.' As of 12 October 2015: https://www.europol.europa.eu/ec/ec3-board
[345] Interview conducted by RAND Europe with the UK NCA.
[346] Example: until October 2015 the US was one of the main cash-out destinations for card-present fraud. This changed when the US implemented EMV standards. See: Gara, Tom. 2014. 'October 2015: The End of the Swipe-and-Sign Credit Card.' *The Wall Street Journal*, 6 February. As of 12 October 2015: http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/
[347] Interview conducted by RAND Europe with the FBI.
[348] Interview conducted by RAND Europe with the FBI.
[349] European Commission. 2010. 'Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats.' *Press Release*, April 14. As of 12 October 2015: http://europa.eu/rapid/press-release_MEMO-11-246_en.htm

cyberincident management, public-private partnerships, raising awareness and cybercrime.[350]

Numerous practical activities have been facilitated within the Working Group, such as the European Network and Information Security Agency's (ENISA) Cyber Atlantic tabletop exercise in November 2011[351] and the launch of the Global Alliance against Child Sexual Abuse Online one year later.[352] The EU-US dialogue also helped spur the development of cybersecurity strategies in several EU Member States as well as the EU itself.[353] However, rather than follow the US in appointing a 'cyber czar', the EU has opted to design joint leadership mechanisms such as Europol's EC3 in 2013.[354]

During the March 2014 Summit in Brussels, the transatlantic partners further committed to opening up an EU-US Cyber Dialogue to enhance the exchange on crosscutting cyber issues.[355] The inaugural meeting was held on 5 December 2014 and considered topics such as international cyberspace developments, the promotion and protection of human rights online, political-military and international security and cybersecurity capacity building.[356]

Among other issues, the current priorities of the Working Group include creating standards for risk management, increasing cybersecurity awareness, promoting the Budapest Convention and managing botnet attacks.[357]

5.3 Operational cooperation: case studies

Besides cooperation at the strategic level, nation states and the private sector have also increased joint efforts at the operational level. EC3, for example, has an embedded liaison officer from the FBI who is stationed in the headquarters on a full-time basis. The case studies that follow have been selected from among many as an indication of how operational cooperation works in practice. They were chosen because they took place during or after 2014 and include stakeholders in the public and private sectors, within and outside the EU.

5.3.1 The Beebone Botnet: Operation Source

In March 2014, the rapid spread of a previously insignificant botnet, now known as Beebone, grabbed the attention of researchers at Intel Security[358] and McAfee Labs.[359] As

[350] White House. n.d.-b. 'FACT Sheet, U.S.-EU Cyber cooperation.' *Office of the Press Secretary*, March 26. As of 12 October 2015: https://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation

[351] According to ENISA, '"Cyber Atlantic 2011" is using simulated cyber-crisis scenarios to explore how the EU and US would engage each other and cooperate in the event of cyber-attacks on their critical information infrastructures.' See: European Union Agency and Information Security (ENISA). n.d. 'First joint EU-US cyber security exercise conducted today.' *Press Release*, 3 November. As of 12 October 2015: https://www.enisa.europa.eu/media/press-releases/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011; European Union Agency for Network and Information Security (ENISA). n.d. 'Cyber Atlantic 2011.' As of 12 October 2015: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011

[352] European Commission. 2012b. 'EU and US launch Global Alliance to fight child sexual abuse online.' *Press Release*, June 21. As of 12 October 2015: http://europa.eu/rapid/press-release_IP-12-680_en.htm

[353] Malmström, Cecilia. 2013. *Next step in the EU-US cooperation on Cyber security and Cybercrime*. Speech at the Homeland Security Policy Institute, George Washington University, 30 April. As of 12 October 2015: http://europa.eu/rapid/press-release_SPEECH-13-380_en.doc

[354] Malmström 2013.

[355] European Union External Action (EEAS). 2014. 'Fact Sheet: EU-US cooperation on cyber security and cyberspace.' *EEAS*, March 26. As of 12 October 2015: http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf

[356] EEAS 2014.

[357] EEAS 2014.

a polymorphic downloader, the AAEH botnet had the ability to change its signature every few hours and functioned as an effective delivery system for other malware, rootkits, ransomware, password stealers and fake anti-virus programs.[360] Additionally AAEH used a Domain Generating Algorithm (DGA) that changed the Internet Protocols (IPs) and domain names of the command and control servers more than five times a month.[361] Curtailing the spread of AAEH primarily necessitated that defenders understood the algorithm behind Beebone's command-and-control infrastructure to determine where it would move next.[362] Due to the AAEH's DGA and polymorphic abilities, it took Intel Security and McAfee almost six months to collect the necessary threat intelligence and to brief law enforcement agencies on how to curtail and take down the Beebone botnet.[363]

In September 2014, McAfee Labs' telemetry identified more than 100,000 AAEH-infected systems in 195 countries, with the majority of infections occurring in the US.[364] In an effort to mitigate the spread of AAEH, security vendors added additional protection layers to their antivirus software, which reportedly pushed down the global number of infected systems to approximately 12,000.[365]

Then on 8 April 2015, an international public-private joint operation, known as *Operation Source*, successfully 'sinkholed' the Beebone botnet by registering, suspending and seizing approximately 100 DGA domain names and redirecting the botnet traffic to secure servers maintained by the Shadowserver Foundation. Based on a US court order, the operation effectively cut the infected systems off from the botnet's command-and-control infrastructure, so stopped the continuous morphing routine and curtailed AAEH's infection rate.[366]

Led by the Dutch National High Tech Crime Unit (NHCTU), the operation included EC3 and its new Joint Cybercrime Action Taskforce (J-CAT),[367] the FBI, the US Attorney's Office for the Southern District of New York and the Computer Crime and Intellectual Property Section (CCIPS) within the US Department of Justice (DoJ).[368]

Additionally, security researchers at Intel Security, McAfee, Kaspersky Lab and Trend Micro provided technical assistance and threat intelligence,[369] while the Shadowserver

---

[358] In 2011, Intel acquired McAfee but the McAfee brand still operates separately from Intel Security

[359] Allan, Darren. 2015. 'Intel spearheaded international effort to down Beebone botnet.' *ITProPortal.com*, April 10. As of 12 October 2015: http://www.itproportal.com/2015/04/10/intel-spearheaded-international-effort-beebone-botnet/

[360] US-CERT. 2015. 'Alert (TA15-098A) AAEH.' As of 12 October 2015: https://www.us-cert.gov/ncas/alerts/TA15-098A

[361] Samani, Raj. 2015. 'Update on Beebone Botnet Takedown.' *McAfee Labs*, April 20. As of 25 September: https://blogs.mcafee.com/mcafee-labs/beebone-update

[362] Lemos, Robert. 2015. 'Joint international Effort Disrupts Beebone Botnet.' *eWeek.com*, April 9. As of 12 October 2015: http://www.eweek.com/security/joint-international-effort-disrupts-beebone-botnet.html

[363] Lemos 2015.

[364] Samani, Raj & Vincent Weafer. 2015. 'Takedown Stops Polymorphic Botnet.' *McAfee Labs*. April 9. As of 12 October 2015: https://blogs.mcafee.com/mcafee-labs/takedown-stops-polymorphic-botnet

[365] Samani & Weafer 2015.

[366] Samani & Weafer 2015.

[367] J-CAT was launched in September 2014 and is located at the Europol headquarters in The Hague, the Netherlands. It functions primarily as a cooperation hub and is composed of cyber liaison officers from seven EU Member States, non-EU law enforcement partners from Colombia, Australia, Canada and the US (represented by the FBI, the Secret Service and ICE) and the EC3.

[368] FBI. 2015b. 'FBI Works with Foreign Partners to Target Botnet.' *Press Release*, April 9. As of 12 October 2015: https://www.fbi.gov/news/pressrel/press-releases/fbi-works-with-foreign-partners-to-target-botnet

[369] Samani & Weafer 2015; Lagrimas, Dianne. 2015. 'Beebone Botnet Takedown: Trend Micro Solutions.' *Trend Micro, Threat Encyclopedia*. As of 12 October 2015: http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions

Foundation offered the operational infrastructure, support and collection of the botnet data.[370]

According to Europol, the data harnessed from the sinkhole is currently being redistributed to ISPs and Computer Emergency Response Teams (CERTs) across the globe, to help and inform victims.[371]

5.3.1.1 Lessons learned: stakeholder cooperation

While Operation Source may have had less effect than anticipated, due to the ability of the Beebone botnet to circumvent countermeasures and displace itself to other geographical regions, the responses to Operation Source indicate how transnational cooperation is imperative in the fight against cybercrime. One interviewee noted that cooperation between the EU and the US is still evolving into a more trusted relationship, and as a result, major takedown operations will increase in the future.[372]

A review of the existing literature on Operation Source provides further lessons on stakeholder cooperation. In Allan (2015), Raj Samani, EMEA CTO at McAfee, recognised that Operation Source functions as additional evidence to demonstrate the necessity to fight cybercrime through a combined, public-private response. In the case of Beebone, law enforcement agencies focused on operation planning and execution, while the private sector delivered threat intelligence and provided the necessary infrastructure to sinkhole the botnet. Samani believes such cooperation offers the best chance of bringing down cybercriminals and preparing against the ever-evolving cyberthreat landscape.[373]

Others echoed Samani's reaction to the Operation. The FBI Assistant Director for Cyber, Joseph Demarest, Jr., indicated that the victimisation caused by Beebone is worldwide and so requires a global law enforcement approach, which includes the FBI, as well as the EC3, the J-CAT and the Dutch National High Tech Crime team.[374] From the European side, Europol's Deputy Director of Operations, Wil van Gemert, expressed similar sentiments as he focused on the global nature of the threat and response to it, as well as the need to cooperate with private industry.[375]

Finally, Paul Gillen, the former Head of Operations at the EC3, stated that the agency would now look at whether those behind the attacks could be identified and brought to justice. He admitted the taskforce's solution was not a permanent one: 'We can't sinkhole these domains forever. We need those infected to clean up their computers as soon as possible.'[376] This introduces another stakeholder into the equation: users. Cooperation between public and private parties is heralded, arguably deservedly so, but users may also need to play an active role in cleaning up their infected machines.

[370] Shadowserver Foundation. 2015a. 'AAEH/Beebone Botnet.' As of 12 October 2015: https://aaeh.shadowserver.org/
[371] Europol. 2015l. 'International Police Operation Targets Polymorphic Beebone Botnet.' *Press Release*, April 9. As of 12 October 2015: https://www.europol.europa.eu/content/international-police-operation-targets-polymorphic-beebone-botnet
[372] Interview conducted by RAND Europe with the FBI.
[373] Allan 2015.
[374] FBI 2015b.
[375] Europol 2015l.
[376] Simmons, Dan. 2015. 'Europol kills off shape-shifting "Mystique" malware.' *BBC*, 9 April. As of 12 October 2015: http://www.bbc.co.uk/news/technology-32218381

5.3.2 BlackShades NET

Since at least 2010, BlackShades, a self-proclaimed information technology (IT) surveillance and security organisation, was selling its software products in numerous underground forums, under the umbrella of 'spying on spouses and children', easing suspicion 'about possibly cheating partners', and overcoming paranoia about 'people using your PC in unwanted ways'.[377]

The organisation's flagship product was BlackShades NET, a malicious and powerful remote access tool (RAT).[378] This threat tool is a variant of malware (see Section 2.7.1). BlackShades' RAT infected computers through multiple attack vectors, such as tricking victims into clicking on a malicious link, using Java exploits, fake torrent downloads, drive-by attacks or by manually installing the software on a victim's computer.[379]

Once a victim was infected, the attacker gained full remote control over the system. The attacker could, for instance, turn on the webcam and microphone to spy on the victim, record keystrokes to obtain passwords, download and encrypt files for blackmail purposes, spread BlackShades through the victim's social network or turn the system into a bot that could be sold to bot-herders on BlackShades' integrated bot marketplace or used to conduct distributed denial of service (DDoS) attacks.[380]

Some have tried to defend BlackShades' DDoS attack functionality by arguing that it was testing personal network defences against such attacks. Although Adam Kujawa, at Malwarebytes.org, notes that this argument would be synonymous with someone building a bomb to see if his house was explosion proof,[381] the legal challenges for criminalising preparatory acts in cyberspace are considerable.

The pricing of BlackShades' RAT was troublesome since it was also geared towards mass consumption and hovered between US$ 40 and US$ 100,[382] which is comparatively cheap for a malicious ready-to-go remote access tool that included ransomware and malware installers, key-loggers, USB infectors, instant messaging spreaders and DDoS attack protocols.[383]

Indeed, BlackShades' RAT went far beyond any existing legal grey area on the issue of remote control. Its conduct is a powerful reminder of how a product can be advertised as having a positive purpose, while actually being deeply harmful. The US DoJ estimates that BlackShades' RAT was purchased by 'thousands of people in more than 100 countries and used to infect more than half a million victim computers'.[384] According to

[377] Kujawa, Adam. 2012. 'You Dirty RAT! Part 2 – BlackShades NET.' *Malwarebytes*, June 15. As of 12 October 2015: https://blog.malwarebytes.org/intelligence/2012/06/you-dirty-rat-part-2-blackshades-net/
[378] Remote access tools can also be used for legitimate purposes such as accessing a work computer from home.
[379] Kujawa 2012.
[380] Eurojust. 2014b. 'International operation hits BlackShades users.' *Press Release*, May 19. As of 12 October 2015: http://www.eurojust.europa.eu/press/pressreleases/pages/2014/2014-05-19.aspx
[381] Kujawa 2012.
[382] Kirk, Jeremy. 2015. 'Swedish man pleads guilty to peddling BlackShades malware.' *CIO*, February 18. As of 12 October 2015: http://www.cio.com/article/2886453/swedish-man-pleads-guilty-to-peddling-blackshades-malware.html
[383] Kujawa 2012.
[384] United States Department of Justice (US DoJ). 2014a. '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.' *Press Release*, May 19. As of 12 October 2015: http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection

Symantec's 2013 telemetry data, India was the country most affected, followed by the US and the UK.[385]

The existence and scope of BlackShades' RAT was uncovered accidentally back in 2012 amid a two-year international law enforcement operation into credit card crimes. In June 2012 the FBI arrested the co-creator of BlackShades' RAT, Michael Hogue, during 'Operation Cardshop',[386] after he boasted that he personally had infected 50–100 computers and that he sold his RAT for just US$ 50 to others who infected thousands of computers with malware.[387] In January 2013, Hogue pleaded guilty to conspiracy to commit computer hacking and the distribution of malware. He is currently facing up to 20 years in prison and is awaiting sentencing in the US.[388]

Despite the arrest of Michael Hogue in 2012, BlackShades not only continued its sales operation but actually expanded and professionalised its services within the underground community.[389] According to the DoJ, Swedish national Alex Yucel, owner and co-creator of BlackShades' RAT, employed several paid administrators, including a marketing director, website developer, customer service manager and a team of customer service representatives, to generate sales of more than US$ 350,000 between September 2010 and April 2014.[390] Alex Yucel was arrested in Moldova and extradited to the US in early 2015.[391] On 23 June 2015 he was sentenced to 57 months in prison and a three-year supervised release.[392]

5.3.2.1 Operation Blackshades

At the time of writing, Operation BlackShades is deemed one of the largest global cyber law enforcement operations ever conducted, based on the number of participating countries. It included police agencies and prosecutors from 19 different countries,[393] as well as EC3, Eurojust and the FBI.

Acting on intelligence the FBI gained from apprehending Michael Hogue and its follow-up investigation into BlackShades, the US Attorney's Office for the Southern District of New York reached out to the Dutch public prosecutor, who in turn approached Eurojust.[394] While the US was primarily focused on taking down BlackShades' European servers, the

---

[385] Symantec. 2013. 'BlackShades Rat Usage on the Rise Despite Author's Alleged Arrest.' *Security Response Blog*, November 25. As of 12 October 2015: http://www.symantec.com/connect/blogs/blackshades-rat-usage-rise-despite-author-s-alleged-arrest

[386] Federal Bureau of Investigation (FBI). 2012. 'Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce 24 Arrests in Eight Countries as Part of International Cyber Crime Takedown.' *New York FBI Office*, June 26. As of 12 October 2015: https://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown

[387] FBI 2012.

[388] US DoJ 2014.

[389] US DoJ 2014.

[390] US DoJ 2014.

[391] According to the FBI, Yucel 'was the first defendant ever to be extradited from Moldova to the United States'. See: FBI. 2015c. 'Co-Creator of BlackShades Malware Pleads Guilty in Manhattan Federal Court.' *Press Release*, February 18. As of 12 October 2015: https://www.fbi.gov/newyork/press-releases/2015/co-creator-of-blackshades-malware-pleads-guilty-in-manhattan-federal-court

[392] FBI. 2015d. 'Swedish Co-Creator of BlackShades Malware That Enabled Users Around the World to Secretly and Remotely Control Victims' Computers Sentenced to 57 Months in Prison.' *Press Release*, June 23. As of 12 October 2015: https://www.fbi.gov/newyork/press-releases/2015/swedish-co-creator-of-blackshades-malware-that-enabled-users-around-the-world-to-secretly-and-remotely-control-victims-computers-sentenced-to-57-months-in-prison

[393] Australia, Austria, Belgium, Canada, Chile, Croatia, Denmark, Estonia, Finland, France, Germany, Italy, Moldova, Slovenia, Sweden, Switzerland, the Netherlands, UK, USA.

[394] Eurojust. 2015b. *Operation BlackShades: An Evaluation*. As of 12 October 2015: https://www.gccs2015.com/sites/default/files/documents/Bijlage%202%20-%20Eurojust%20(10%2004%2015)%20Blackshades-Case-Evaluation.pdf

European law enforcement agencies were interested in apprehending the creators, sellers and users of BlackShades' RAT.[395]

The Netherlands opened a case in November 2013 and subsequently organised four coordination meetings with numerous law enforcement agencies from across Europe.[396]

Apart from the US, only representatives from the EU Member States were explicitly mentioned as taking part in the first coordination meeting. Other countries, however, were involved in the overall operation and demonstrated interest in participating by contacting officials already involved in the operation.[397] Eurojust had an overview of countries involved.[398] It is important to note that significant capacity is required for countries to be involved in an operation of this type, meaning that it is unlikely every country was willing to do something or had the legal capabilities to do so.[399] For example, representatives at Eurojust were aware that Canada and Chile were willing and able to cooperate.[400] According to Eurojust, the objective of the first meeting was to 'ascertain which states could take judicial measures against identified subjects'.[401] In the following three meetings, the investigation efforts of the participating states were aligned and information shared to overcome the different national legal hurdles of either opening a criminal case or enriching data that were already available.[402]

Operation BlackShades was based on a simple two-step strategy: first, dismantle the BlackShades organisation and second, take down all the Command and Control (C&C) servers to stop sales of the software.[403]

The two-day operation started on 13 May 2014. All in all, 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. During the operation substantial quantities of cash, illegal firearms and drugs were also found and seized.[404]

According to the Dutch Public Prosecutor's office (OM), the Dutch police raided 34 addresses in the Netherlands. While no one was arrested, the police confiscated numerous computers and hard disks.[405] In Germany 111 addresses were raided and 150 criminal cases opened.[406] In Austria the police conducted 21 raids and arrested 28 suspects.[407] And in the UK 17 were arrested.[408] In the US, the FBI's 40 field offices conducted 'approximately 100 interviews, executed more than 100 email and physical

[395] Eurojust 2015b.
[396] Eurojust 2015b.
[397] Interview conducted by RAND Europe with Europol.
[398] Interview conducted by RAND Europe with the Assistant to the Dutch Desk for the Netherlands at Eurojust.
[399] Interview conducted by RAND Europe with the Assistant to the Dutch Desk for the Netherlands at Eurojust.
[400] Interview conducted by RAND Europe with the Assistant to the Dutch Desk for the Netherlands at Eurojust.
[401] Eurojust 2015b.
[402] Eurojust 2015b.
[403] Eurojust 2015b.
[404] Europol. 2014c. 'Worldwide Operation against Cybercriminals.' *Press Release*, May 19. As of 12 October 2015: https://www.europol.europa.eu/content/worldwide-operation-against-cybercriminals
[405] Openbaar Ministerie. 2014. 'Wereldwijde actie politie en justitie tegen hackers.' *Landelijke Parket*, May 19. As of 12 October 2015: https://www.om.nl/vaste-onderdelen/zoeken/@85963/wereldwijde-actie/
[406] Heise Online. 2014. 'Ermittlungen wegen "BlackShades" -Trojaner in Deutschland.' *Heise Online*, May 22. As of 12 October 2015: http://www.heise.de/newsticker/meldung/Ermittlungen-wegen-Blackshades-Trojaner-in-Deutschland-2195984.html
[407] Bundeskriminalamt (BKA). 2014. 'EUROPOL-Operation "BlackShades": 19 Tatverdächtige in Österreich ausgeforscht.' *Press Release*, May 20. As of 12 October 2015: http://www.bmi.gv.at/cms/BK/presse/files/2052014_BlackShades.pdf
[408] BBC. 2014. 'BlackShades: Arrests in computer malware probe.' *BBC*, May 19. As of 12 October 2015: http://www.bbc.com/news/uk-27471218

search warrants and seized more than 1,900 domains used by BlackShades users to control victims' computers'.[409]

Among those arrested in the US were BlackShades' adminstrator Brendan Johnson, who was subsequently sentenced to one year and a day in prison and BlackShades' customers Marlen Rappa, who received the same sentence, and Kyle Fedorek, who was sentenced to two years.[410]

During the operation Eurojust was responsible for coordinating and delivering status overviews of the country-specific investigations as well as for providing judicial assistance.[411] EC3 provided real-time analytical support and was involved in the follow-up and identification of the victims, as well as the promotion of technical solutions to guard against the spread of BlackShades' RAT.[412]

Reports also suggested that Paypal and Microsoft were cooperating with the FBI. In an article on The Hacker News website, Wang Wei noted that the FBI was primarily pursuing all those who purchased BlackShades through Paypal.[413] According to the indictment against Kyle Fedorek, the government obtained a search warrant for the BlackShades hotmail account (blackshadessupport@hotmail.com), which allowed the FBI access to BlackShades' customer database.[414]

The Dutch Public Prosecutor's office revealed that the NHTCU also hacked into BlackShades' servers before 13 May to gather evidence and intelligence about the organisation.[415] The NHTCU's conduct has been subsequently questioned by the Dutch Parliament.[416] The Dutch Ministry of Security and Justice defended the NHTCU by elaborating that, based on Article 125i of the Dutch Criminal Code of Procedure, the police received authorisation from an investigative magistrate (*rechter-commissaris*) to enter the BlackShades' server, the physical location and ownership of which was unknown at the time and which was deemed to be connected to an ongoing serious crime.[417]

5.3.2.2 Lessons learned: Eurojust

The literature shows that Eurojust identified several lessons learned during Operation BlackShades. First, given the speed with which news spreads on the Internet, synchronising the timing of searches, seizures and arrests is very important, particularly when it concerns global operations. Second, collecting information on the victims and the financial losses caused by the malware is important to support criminal procedures, especially in the US, where cases are victim and loss driven. Third, repressive measures ought to be combined with high-volume enhanced prevention, such as warning emails

[409] FBI. 2014. 'International Blackshades Malware Takedown.' *Press Release*, May 19. As of 12 October 2015: https://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown
[410] FBI 2015c.
[411] Eurojust 2015b.
[412] Eurojust 2015a.
[413] Wei, Wang. 2014. 'FBI raids BlackShades RAT Malware Customers in Europe and Australia.' *HackerNews*, May 16.' As of 12 October 2015: http://thehackernews.com/2014/05/fbi-raids-blackshades-rat-malware_16.html
[414] US DoJ. 2014b. *United States of America v. Kyle Fedorek*. As of 12 October 2015: http://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Blackshades,%20Fedorek%20Complaint%2014%20Mag.%201064_0.pdf
[415] Openbaar Ministerie 2014.
[416] Rijksoverheid. 2014. *Antwoorden Kamervragen over het hacken van servers door de politie*. As of 17 October 2014: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/10/18/antwoorden-kamervragen-over-het-hacken-van-servers-door-de-politie-terwijl-de-zogenaamde-hackwet-nog-niet-door-de-kamer-is-beha
[417] Rijksoverheid 2014.

and letters, as well as visits by law enforcement, to deter lower-level purchasers from further involvement in cybercrime.[418] Troels Oerting, Head of the EC3 at Europol at the time, said:

> *This case is yet another example of the critical need for coordinated law enforcement operations against the growing number of cybercriminals operating on an EU and global level. EC3 will continue – together with Eurojust and other partners – to work tirelessly to support our partners in the fight against fraudsters and other cybercriminals who take advantage of the Internet to commit crime. The work is far from over, but our cooperation to work together across borders has increased and we are dealing with cases on an ongoing basis*.[419]

Koen Hermans, Assistant to the National Member for the Netherlands, echoed these comments when he stated: 'The number of countries involved in this operation has shown the inherent value in Eurojust's coordination meetings and coordination centres.'[420]

5.4 Remaining challenges in transnational cooperation

Despite the many (recent) successes and the continuous improvement of transnational cooperation, challenges remain. This section focuses on challenges identified by individuals interviewed for the purposes of this study. Wherever possible, interviews were supplemented by targeted searches for relevant literature.

5.4.1 Mutual Legal Assistance Treaties

Due to the internationalisation of cybercrime evidence, law enforcement agencies are forced to conduct their investigations by requesting electronic communications and other data records from countries that are beyond their jurisdictional reach. The legal process through which law enforcement agencies request and compel foreign data disclosure is called the Mutual Legal Assistance Treaty (MLAT).[421]

Processing an MLAT request is both time-intensive and cumbersome as it requires a sequence of linear steps within two administrative and legal processes.[422] An MLAT request can be delayed further if national legislation requires that MLATs are sent via traditional postal services[423] or if governments do not provide online submission forms.[424] In the United Kingdom (UK), for instance, an MLAT request for communication data can take between eight and 13 months.[425] In the US the average is around 10 months.[426] Unsurprisingly, the Global Network Initiative therefore concluded in its 2015

[418] Eurojust 2015b.
[419] Europol 2014b.
[420] Eurojust 2014b.
[421] US DoJ. 2015b. *FY 2015 Budget Request – Mutual Legal Assistance Treaty Process Reform*. As of 12 October 2015: http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf
[422] Kent, Gail. 2014. 'Sharing Investigation-specific data with law enforcement – an international approach.' *Stanford Public Law Working Paper*, As of 12 October 2015: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413
[423] Kent 2014.
[424] White House.2013b. *Liberty and Security in a Changing World – Report and Recommendations of the President's Review Group on Intelligence and Communication Technologies*. As of 12 October 2015: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
[425] Kent 2014.
[426] White House 2013b.

report that the MLAT process is inefficient as the time required is 'measured in months and in some cases years'.[427]

The problems surrounding the MLAT process were confirmed by the interviewees, who stressed the need for a comprehensive reform to streamline the flow of information between law enforcement agencies and governments.[428] When it comes to cyberfraud in particular, criminals currently benefit from the slow response time of transnational cooperation on the one hand and the rapid transfer of money to 'safe havens' abroad on the other.[429]

Despite these well-known challenges surrounding the MLAT process and ongoing initiatives to modernise the process by the Council of Europe (CoE) and the United Nations Office on Drugs and Crime (UNODC), the European Commission (EC) did not make MLAT reform part of its 2015 Agenda on Security. Instead the EC seems to be focusing on the possible development of other bilateral or multilateral agreements with other countries to replace MLATs altogether.[430]

Given the cumbersome nature of the current MLAT process, law enforcement agencies have sought numerous ways to facilitate more effective transnational cooperation outside the MLAT framework. The Joint Cybercrime Action Taskforce (J-CAT), hosted by Europol's EC3, is one project that has brought together cyberliaison officers from various EU Member States and non-EU law enforcement partners from Australia, Canada, Columbia and the US (which is represented by a liaison officer from the FBI and the United States Secret Service).

Within the MLAT context, the J-CAT works as a coordinating hub to exchange strategic information and provides a face-to-face platform to discuss and facilitate MLAT requests.[431]

In addition to the J-CAT, two or more EU Member States can choose to set up so-called Joint Investigation Teams (JITs), which allow for the sharing of investigative information without the passing of MLATs.[432] According to one interviewee, the FBI is only able to participate in a JIT as an associate member due to current constraints imposed by the US DoJ. This means the FBI is unable to take full advantage of the benefits of the JIT.[433]

5.4.2 Data retention

Attempts to obtain information from a number of counties to inform investigations into cybersecurity can be challenged by national data retention times. Law enforcement agencies need to collect digital trace evidence, such as Internet Protocol (IP) addresses,

[427] Global Network Initiative. 2015. *Data Beyond Borders – Mutual Legal Assistance in the Internet Age*. As of 12 October 2015: http://csis.org/files/attachments/GNI%20MLAT%20Report.pdf
[428] Interview conducted by RAND Europe with the FBI, Europol, the Reykjavik Metropolitan Police (LRH), Office of the Special Prosecutor (ESS) (Iceland), and the National Commission of the Icelandic Police (RLS).
[429] Interview conducted by RAND Europe with the Reykjavik Metropolitan Police (LRH), the Office of the Special Prosecutor (ESS) and the National Commission of the Icelandic Police (RLS); Global Conference on Cyberspace (GCCS). 2015. *Chair's Statement*. As of 12 October 2015: https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf
[430] European Commission. 2015. *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions – The European Agenda on Security*. COM (2015) 185 Final. As of 12 October 2015: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
[431] Interview conducted by RAND Europe with Europol.
[432] Interview conducted by RAND Europe with the FBI; Europol. n.d.-b. 'Joint Investigation Teams (JITs).' As of 12 October 2015: https://www.europol.europa.eu/content/page/joint-investigation-teams-989
[433] Interview conducted by RAND Europe with the FBI.

to start an investigation. But if these data have not been retained there is no digital trace evidence to collect and it becomes almost impossible for investigators and prosecutors to initiate an investigation and compile a solid legal case against a cybercriminal.[434]

The decision by the Court of Justice of the European Union (CJEU) to invalidate the Data Retention Directive on 8 April 2014 (C-293/12 & C-594/12) [435] prompted mixed responses from all parties concerned. The Court reasoned that 'although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary'.[436] In other words, even if the Directive qualified as being necessary, it failed to meet the proportionality requirement.

The CJEU perceived five elements as particularly problematic. First, the Directive authorised blanket retention for 'all individuals, all means of electronic communications, and all traffic data without any differentiation, limitation, or exception'.[437] Second, the Directive did not identify substantive and procedural conditions under which national competent authorities can justify their access to data. Third, the Directive allowed a retention period of a minimum of six months and a maximum of 24 without distinction about the types of data and the purpose of their retention. Fourth, the Directive lacked sufficient safeguards against the risk of abuse, largely because it failed to ensure the irreversible destruction of data after the retention period. Finally, the Directive did not require data to be retained within the EU, complicating jurisdiction over the data and creating loopholes in compliance control.

As each Member State reacted differently to the CJEU ruling, the invalidation of the Data Retention Directive created severe repercussions for the daily work of law enforcement agencies fighting cybercrime.[438] The courts in Austria, Bulgaria and the Netherlands, for instance, declared the Directive unconstitutional and annulled their national data retention laws.[439] As a result, ISPs in those countries stopped retaining data and started deleting them.[440] By contrast, in the Czech Republic and Denmark the data retention laws were interpreted as being in compliance with the CJEU ruling.[441] The UK High Court struck down the Data Retention and Investigatory Powers Act (DRIPA) in July 2015, although it will remain in effect until March 2016.[442]

---

[434] Interview conducted by RAND Europe with the Assistant to the Dutch Desk for the Netherlands at Eurojust; Europol.
[435] Court of Justice of the European Union. 2014. 'The Court of Justice declares the Data Retention Directive to be invalid.' *Press Release* No 54/14, April 8. As of 12 October 2015: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf
[436] Court of Justice of the European Union 2014.
[437] Court of Justice of the European Union 2014.
[438] Interview conducted by RAND Europe with the Assistant to the Dutch Desk for the Netherlands at Eurojust; Europol.
[439] Council of Europe. 2015b. *Assessment report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime*. Cyber Crime Convention Committee, June 21. As of 12 October 2015: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b; Open Rights Group. 2015. *Data retention in the EU following the CJEU ruling – updated April 2015*. As of 12 October 2015: https://www.openrightsgroup.org/assets/files/legal/Data_Retention_status_table_updated_April_2015_uploaded_finalwithadditions.pdf
[440] Open Rights Group 2015.
[441] Council of Europe 2015b; Open Rights Group 2015.
[442] Bowcott, Owen. 2015. 'High court rules data retention and surveillance legislation unlawful.' *The Guardian*, 17 July. As of 12 October 2015: http://www.theguardian.com/world/2015/jul/17/data-retention-and-surveillance-legislation-ruled-unlawful

Together with the differences in the type of data law enforcement agencies need in the context of an investigation – subscription, traffic, location and content data – the increasingly fragmented data retention landscape has complicated law enforcement activities. The Council of Europe therefore stressed in June 2015, that 'preservation measures are particularly important at a time when procedural law powers and regulations on data retention are uncertain and where questions arise regarding jurisdiction in the context of cloud computing'.[443]

According to the Assistant to the Dutch Desk for the Netherlands at Eurojust, prior to the CJEU's decision some national law enforcement agencies had complained that data were being stored for only six months. In some countries today no data are being stored at all, which makes it almost impossible to launch some investigations.[444] Similar concerns were echoed by the interviewees from Europol, who explained that the current national data retention times are sometimes insufficient for the information to be reported from a local to a national level, where a decision has to be taken on whether the information is criminal in nature and connected to a serious crime, before it can be passed on to the liaison bureau or Europol.[445]

From the law enforcement perspective, unclear and relatively short retention times translate into weakening transnational cooperation efforts and hamper law enforcement agencies' efforts to understand how cybercriminal networks operate and evolve in cyberspace over time.[446]

According to the interviewees the minimum data retention time ought to be informed by investigative requirements, which currently suggest that a minimum retention period of several months is desirable.[447] This assessment largely converges with the EC's 2011 evaluation report on the Data Retention Directive.[448] It also acknowledges the EP's call to strike the right balance on data retention times while applying the principles of proportionality, necessity and legality and including appropriate safeguards of accountability and judicial redress.[449] Finding a consistent approach towards data retention across the EU must therefore reconcile the need for a harmonised and coherent approach to law enforcement processes, while ensuring a high level of respect for privacy and the protection of personal data.

5.4.3 Deconfliction and avoiding duplication

Deconfliction is an essential element of the cross-national coordination of law enforcement activities to fight transnational cybercrime. The aim of deconfliction is to prevent duplication of efforts and to avoid the accidental targeting of other law enforcement operations.[450] In this respect the exchange of information and intelligence across borders and among agencies is key to formulating a practical and coordinated response to the different levels of a cybercriminal network. Deconfliction works at both ends of the information chain. At the national level, agencies and ministries have to

[443] Council of Europe 2015b.
[444] Interview conducted by RAND Europe with the Assistant to the Dutch Desk for the Netherlands at Eurojust.
[445] Interview conducted by RAND Europe with Europol.
[446] Interview conducted by RAND Europe with Europol.
[447] Interview conducted by RAND Europe with Europol.
[448] European Commission. 2011. *Report from the Commission to the Council and the European Parliament - Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*. COM (2011) 225 Final. As of 12 October 2015: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF
[449] European Parliament. 2015b. *Resolution on the European Agenda on Security*. 2015/2697(RSP), July 9. As of 12 October 2015: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2015-0269&format=XML&language=EN
[450] Interview conducted by RAND Europe with the UK National Crime Agency (NCA).

coordinate their responses on the ground while aiming to fulfil the legal requirements for prosecuting cybercriminals on their own soil. At the international level, EC3's J-CAT provides a focal point that allows the various liaison officers to exchange strategic information quickly, facilitates cross-border cooperation and serves as an information hub on any given action day. Only if these deconfliction mechanisms are used to the full extent possible can cybercrime be tackled in an impactful and comprehensive manner. This is also evidenced by actions that have been carried out unilaterally led to criticism.

As an example of what can happen when actors fail to deconflict, in March 2012 Microsoft launched Operation b71, which started with an ex parte temporary restraining order filed with the US District Court for the Eastern District of New York, against 39 low-level John Does[451] and two data centres.[452] Microsoft, in cooperation with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the National Automated Clearing House Association (NACHA), alleged that the servers and domains hosted by Continuum Data Centers LLC. and BurstNet were part of the Zeus botnet C&C infrastructure.[453]

On 23 March, escorted by US Marshalls, Microsoft, FS-ISAC and NACHA executed a coordinated physical seizure of the C&C servers to gain data and virtual evidence for a criminal case against the botnet operators.[454]

Criticism of Operation b71 was voiced by Fox-IT – an information security company located in the Netherlands – which alleged that Microsoft 'endangered the success of countless ongoing investigations by acting unilaterally upon data supplied by core members of the security community who had placed certain restrictions on the use of the information.[455] In fact, a number of the low-level John Does Microsoft named in its civil suit were part of a core group the US DoJ considered to be responsible for numerous operations that have cost businesses millions of dollars in the past few years.[456] Fox-IT therefore noted, 'From our end we can confirm that this information was never supplied for the purposes that Microsoft used it for.'[457] Rik Ferguson, Vice President for Security Research at TrendMicro, added to this by stating that the revelation of the 39 online usernames was not a good idea, as those subjects were now fully aware of the investigation and highly likely to disappear.[458]

All in all, many experts considered that Microsoft's unilateral action went against the collaborative workgroup model that facilitates the sharing of information between the security industry, research organisations and law enforcement agencies.[459] As one interviewee noted, Microsoft failed to deconflict with law enforcement and its peers to provide a long-term solution based on mitigating loses and cleaning up victims'

[451] John Does: individuals whose name or identity is unknown.
[452] United States District Court, Eastern District of New York. 2012. *Microsoft Corp., FS-ISAC INC., and National Automated Clearing House Association v. John Does 1-39*. As of 12 October 2015: http://www.zeuslegalnotice.com/images/Ex_Parte_Application.pdf
[453] United States District Court, Eastern District of New York 2012.
[454] Meisner, Jeffrey. 2012. 'Microsoft and Financial Services Industry Leaders target Cybercriminal Operations form Zeus Botnets.' *Microsoft News Center*, 25 March. As of 12 October 2015: http://blogs.microsoft.com/blog/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets/
[455] Sandee, Michael. 2012. 'Critical analysis of Microsoft Operation B71.' *Fox-IT International Blog*, 12 April. As of 12 October 2015: http://blog.fox-it.com/2012/04/12/critical-analysis-of-microsoft-operation-b71/
[456] Krebs, Brian. 2012. 'Microsoft Responds to Critics over Botnet Bruhaha.' *KrebsonSecurity*, 16 April. As of 12 October 2015: http://krebsonsecurity.com/2012/04/microsoft-responds-to-critics-over-botnet-bruhaha/
[457] Sandee 2012.
[458] Ferguson, Rik. 2012. 'Don't be dumb, keep schtumm.' *TrendMicro Blog*, March 27. As of 12 October 2015: http://countermeasures.trendmicro.eu/dont-be-dumb-keep-schtumm/
[459] Sandee 2012.

computers while coordinating arrests globally.[460] Not surprisingly, Microsoft was eventually accused by a significant number of security researchers of conducting a publicity stunt that was aimed at capturing media headlines and did little or nothing to facilitate the long-term success of law enforcement.[461]

5.5 Recommendations for improving transnational cooperation

The previous section identified challenges remaining in transnational cooperation. Drawing from the insights gained from the case studies and the interviews, this section makes recommendations for improvement in transnational cooperation, focusing on public-private partnerships and the dissemination of digital evidence to be used in court.

5.5.1 Public-private partnerships

Multiple interviewees stressed the need for a structural approach towards public-private partnerships as they are an invaluable source of technical expertise and up-to-date threat intelligence.[462] However, one of the largest obstacles to fostering public-private partnerships is the absence of a single contact point within the law enforcement community that private companies can leverage to share their information with.[463] Currently the legal framework is rather cumbersome, given that private companies have first to identify a particular Member State on the basis of several criteria in relation to the information they want to share. That information then travels from the Member State to Europol and from there on to all the other Member States.[464] The interviewees were clear that they felt that this approach does not work well in the field of cybersecurity. If, for instance, a private company uncovers a long list of stolen credit card numbers, it has no idea which country it is supposed to approach, given that the nationalities of the victims are unknown.[465]

In March 2013, the European Commission published the proposed regulation on the European Union Agency for Law Enforcement Cooperation and Training (to give Europol its full title).[466] In Recital 24 of this proposal, the Commission stipulates that 'Europol should maintain cooperative relations with […] private parties to the extent required for the accomplishment of its tasks'.[467] Yet, the proposed regulation fails to address the problem identified by Europol officials; Article 32 reads:

---

[460] Interview conducted by RAND Europe.
[461] Krebs 2012.
[462] Interviews conducted by RAND Europe with Europol, the Assistant to the Dutch Desk for the Netherlands at Eurojust, the FBI, the UK National Crime Agency (NCA), the Reykjavik Metropolitan Police (LRH), the Office of the Special Prosecutor (ESS) (Iceland) and the National Commission of the Icelandic Police (RLS); Law Enforcement and Prosecutors Conference on Cyber Crime. 2015. Joint Conference Paper. *LEAP2015*, 15 April. As of 12 October 2015: https://www.gccs2015.com/sites/default/files/documents/JOINT%20CONFERENCE%20PAPER%20LEAP2015final.doc
[463] Interview by RAND Europe with Europol.
[464] Interview by RAND Europe with Europol.
[465] Interview by RAND Europe with Europol.
[466] Following the opposition of the European Parliament and the Council to the Commission's proposal to incorporate CEPOL into Europol, the idea of a merger was shelved. See: Council of the European Union. 2015d. 'CEPOL: Council and Parliament agree on updated rules.' *Press Release* 544/15, 30 June. As of 12 October 2015: http://www.consilium.europa.eu/en/press/press-releases/2015/06/30-cepol-updated-rules/
[467] European Parliament. 2014b. *Legislative resolution of 25 February 2014 on the proposal for a regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA*. P7_TA(2014)0121 (COM(2013)0173 – C7-0094/2013 – 2013/0091(COD)). As of 12 October 2015: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0121&language=EN&ring=A7-2014-0096

In so far as necessary for Europol to perform its tasks, Europol may process personal data originating from private parties on condition that they are received via:

(a) a national unit of a Member *State in accordance with national law.*

(b) the contact point of a third country with which Europol has concluded a cooperation agreement in accordance with Article 23 of the Decision 2009/371/JHA prior to date of application of this Regulation.

(c) *an authority of a third country or an international organisation with which the Union has concluded an international agreement pursuant to Article 218 of the Treaty*.[468]

During its first reading, the EP amended this to:

In so far as necessary for Europol to perform its tasks, Europol may process personal data originating from private parties on condition that ***they are not*** *received* ***directly from the private parties but only*** *via:* […][469]

Other passages in the proposed regulation limit Europol's ability to acquire potentially relevant information. Article 32, paragraph 3, for example, states that 'Europol shall not contact private parties directly to retrieve personal data'. And Article 33, paragraph 3, states that 'Europol shall not contact private persons directly to retrieve information'.[470] The EP amended these provisions by removing 'directly', thus proscribing any contact at all. If passed into law this may result in even fewer possibilities of acquiring information and potentially restrict cooperation further.

Interviewees report that the restrictions were particularly troublesome for the operational work of the EC3 and undermined the mission of Europol's newly established Internet Referral Unit (IRU), whose function is to help Member States, in cooperation with industry partners, to identify and remove violent extremist content online.[471] Thus the practical results of the EP's desire to implement 'overall supervision of Europol's processing of personal data, enhancing access rights to personal data, [and] further specifying the uses of personal data'[472] would, in the interviewees' opinion, effectively undermine Europol's mandate to maintain cooperative relations with private parties as set forward in Recital 24.[473]

The draft position of the Council is in part an attempt to accommodate the operational needs of the law enforcement community, by allowing Europol to receive directly personal data from private parties for which the National Unit or contact point cannot be identified in the first instance. However, the limitations set out in the Council's position

[468] European Parliament. n.d. 'Procedure file: 2013/0091 European Union Agency for Law Enforcement Cooperation and Training (Europol).' As of 12 October 2015: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0091(COD)
[469] European Parliament 2014b.
[470] European Parliament 2014b.
[471] Council of the European Union. 2015c. *EU Internet Referral Unit at Europol – Concept note*. As of 12 October 2015: http://data.consilium.europa.eu/doc/document/ST-7266-2015-INIT/en/pdf; Europol. 2015m. 'Europol's Internet Referral Unit to combat terrorist and violent extremist propaganda.' *Press release*, 1 July. As of 12 October 2015: https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda
[472] Weidenholzer, Josef. 2014. 'European Union Agency for Law Enforcement Co-operation and Training (Europol).' *S&D Newsroom*, 24 February. As of 12 October 2015: http://www.socialistsanddemocrats.eu/content/european-union-agency-law-enforcement-co-operation-and-training-europol
[473] European Parliament 2014b.

on Article 32(3a), still severely constrain Europol from transferring any personal data to private parties as required for the purposes of the IRU.[474]

> *Europol may not transfer personal data to private parties except where […]:*
> *(a) the transfer is undoubtedly in the interests of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such a consent; or*
> *(b) the transfer is absolutely necessary in the interests of preventing imminent danger associated with crime or terrorist offences.* [475]

Therefore, according to the interviewees at Europol, the Council is looking into amending Article 32 further, so that it will include all the necessary data protection safeguards, while allowing Europol to fulfil its mandate.[476]

5.5.2 Dissemination of digital evidence to be used in court

One of the challenges in transnational cooperation identified by the interviewees is exchanging data back and forth between agencies and countries with the objective of disseminating information for court purposes.[477] For instance, transition of evidence from one holder to another in cross-border investigation, as well as timeliness and legal challenges, can determine admissibility and the weight of evidence in court. Due to different national data retention times, by the time some elements of the digital evidence are received by law enforcement agencies, other parts may have become legally inaccessible by public prosecution.[478] Besides, different legal requirements for opening up criminal cases and a lack of standardisation in MLAT requests mean that cooperation between the police and the prosecutors must take place at a very early stage in the investigation.[479]

Adapting law enforcement reaction times, either by streamlining or standardising the MLAT request process, and finding innovative ways to enlarge and support the J-CAT and JIT projects within Europol's EC3, would be a positive step forward in the view of interviewees and others writing in this field.

5.6 Conclusion

This chapter has focused on transnational cooperation in the fight against cybercrime. From strategic cooperation through, for example, the EU-US working group, to operational cooperation through actions such as Operation Source and BlackShades, there is broad recognition of the merits of working together with different stakeholders in both the public and the private sphere.

Some examples of successful cooperation have been reported in the media in recent years. However, challenges remain. Interviews conducted by the research team highlighted some of these.

---

[474] Council of the European Union. 2014b. *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA (First reading)*. As of 12 October 2015: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010033%202014%20INIT
[475] Council of the European Union 2014b.
[476] Interview by RAND Europe with Europol.
[477] Interview by RAND Europe with the FBI.
[478] Interview by RAND Europe with the FBI.
[479] Interview by RAND Europe with the Assistant to the Dutch Desk for the Netherlands at Eurojust.

The MLAT process has been identified as outdated and as a hurdle for the effective acquisition of information. Developments with respect to the data retention directive have also complicated matters for law enforcement purposes.

EU policymakers face the challenge of finding a workable balance between safeguarding personal information and allowing law enforcement agencies to protect the public efficiently from cybercriminal activities. Finding this balance matters not only in the context of public-private partnerships; it is also at the heart of issues of data retention and the exclusion of EU law enforcement agencies from the NIS Directive (see Chapter 6).

A final barrier relates to the challenges in facilitating the flow of information across and within countries between the private sector, the police and the prosecution. Interviewees have called for greater harmonisation to facilitate closer cooperation and warned against any policy measures that could lead to greater compartmentalisation and fragmentation. At the same time it is eminently important that closer cooperation between the three entities is based on a lawful and proportional footing and does not harm or infringe upon fundamental human rights and personal data.

6 EFFECTIVENESS OF THE EU RESPONSE

KEY FINDINGS

- The effectiveness of the European Union's response to cybersecurity is difficult to gauge since the concept is challenging to operationalise and measure. The EU approach is still being developed.
- Fragmentation, while lessening, is potentially exacerbated through the exclusion of law enforcement from key provisions of the proposed NIS Directive.
- Capability gaps and differences of priorities with regard to cybersecurity among Member States remain a problem and may hamper the effectiveness of the EU response.
- The current draft of the NIS Directive has proposed a change in the regulatory environment from the currently voluntary and informal approach to securing cooperation between actors in the cybersecurity field, to a mandatory and formal approach. Views differ as to whether this will enhance or reduce the effectiveness of the EU response to cybersecurity.
- The US provides a possible model for enhancing public discourse and awareness, which have been relatively weak in the EU.

6.1 Introduction

Prior to the introduction of the European Union (EU) Cyber Security Strategy (the Strategy) and the accompanying proposal for a Network and Information Security (NIS) Directive in 2013, the European Commission had recognised the ineffectiveness of the EU approach taken so far. Specifically, the Commission stated that:

> *There is currently no effective mechanism at EU level for effective cooperation and collaboration and for trusted information sharing on NIS incidents and risks among the Member States. This may result in uncoordinated regulatory interventions, incoherent strategies and divergent standards, leading to insufficient protection against NIS across the EU.*[480]

The main focus of the EU strategy (as articulated in the proposed NIS Directive) therefore appears to address the challenges caused by fragmentation, both in terms of operational gaps within and among Member States, as well as different opinions on the regulatory approach. According to Ryan et al., the Commission articulated similar concerns as far back as 2001.[481] As we will show, however, EU regulatory measures in the area of cybersecurity have remained largely sector-focused and fragmented, resulting in gaps in cybersecurity regulation. This chapter will address these issues in light of the current debate surrounding the proposed NIS Directive.

It is difficult to make a definitive assessment of the effectiveness of the EU response. First, the issue of how to measure the effectiveness of cybersecurity efforts is open to

[480] 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*. COM (2013) 48 Final - 2013/0027 (COD). As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0048

[481] Pearse, Ryan, Buckenham, Paddy & Donnelly, Niall. 2014. *EU Network and Information Security Directive: Is It Possible to Legislate For Cyber Security?* Arthur Cox, Group Briefing. As of 12 October 2015: http://www.arthurcox.com/wp-content/uploads/2014/10/Arthur-Cox-EU-Network-and-Information-Security-Directive-October-2014.pdf

discussion. For instance, the continued occurrence of cybersecurity incidents, vulnerabilities and threats could be interpreted as an indicator that the EU response is ineffective. This, however, would be an inaccurate conclusion to draw; security, especially cybersecurity, is inherently relative rather than absolute and should be assessed in light of the growing size of the Internet community. Absolute indicators such as the number of incidents fail to demonstrate the true level of threat, when interpreted in isolation.

Second, if effectiveness cannot be reliably measured based on outcomes, then input (i.e. capabilities) becomes the next best indicator of effectiveness. However, this is equally complicated. Reflecting on the EU's attention to capability building, Dunn Cavelty asks, 'Are these approaches sufficient to ensure the necessary level of cyberresilience in Europe? In theory, yes: the European approach to cybersecurity could be considered a best-practice approach, at least on paper. In practice, however, cybersecurity or rather, cyberresilience is very hard to obtain.'[482]

Given these caveats, this chapter focuses primarily on identifying expert perceptions – expressed in commentary pieces, media sources and interviews conducted by the research team on the level of effectiveness of the EU approach so far, and in particular, the proposed NIS Directive. For the purposes of this chapter, 'effectiveness' will be construed as whether, from the perspective of various stakeholders, the agencies and laws operate as envisioned, and what functional challenges they have faced.

While recognising the limitations of subjective perceptions as an evidence base, three themes emerged from our review.

- First, fragmentation exists within the EU in respect of coordination between agencies and identifying and addressing capability gaps among Member States, as well as implementation challenges.
- Second, there are different views as to whether an informal or formal approach to securing the involvement of key actors in cybersecurity is likely to be most effective. Different opinions are presented alongside their justifications.
- Third, there is a recurring issue of scope, in terms of whom the Directive applies to, the definitional challenges it comprises and the sources of its contentions.

Drawing on the US experience, the chapter also takes a comparative approach and identifies overall lessons for the EU.

6.2 Fragmentation is still present but improvement is discernible

Fragmentation was a key characteristic of the EU approach to cybersecurity and was the main incentive for devising the Strategy. As Robinson et al. note:

> *Understanding how coordination and cooperation is achieved in the European cybersecurity policy puzzle is very complex. No one currently has a clear understanding of how all the different pieces fit together. There are many institutions, each working on a specific part of the problem.*[483]

[482] Dunn Cavelty, Myriam. 2013b. 'A Resilient Europe For An Open, Safe and Secure Cyberspace.' *UI Occasional Papers*, No. 23. As of 12 October 2015: http://www.ui.se/eng/upl/files/99632.pdf

[483] Robinson, Neil, Horvath, Veronika, Cave, Jonathan, Roosendaal, Arnold & Klaver, Marieke. 2013. *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts*. European Parliament, Directorate-General for Internal Policies – Policy Department A: Economic and Scientific Policy. As of 12 October 2015: http://www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE_NT(2013)507476_EN.pdf

Chapter 3 provided an overview of the main institutions and agencies involved and the roles they play in the area of cybersecurity but the development of a comprehensive understanding of how the different elements operate together remains challenging. Fragmentation is not necessarily a preventable aspect of cybersecurity policy. As explained in the introductory chapter, the issue of cybersecurity involves a variety of different stakeholders with a range of perspectives. To an extent, any approach to cybersecurity will be marked by some fragmentation and will have to negotiate potentially competing interests. Placing the claims about fragmentation in perspective, Dunn Cavelty notes:

> *Despite a relatively fragmented policy set-up, the EU's strategy for internal cyberresilience cannot be criticised for its fundamentals. A rather pragmatic, level-headed approach has emerged over the years.*[484]

6.2.1 Evidence of reduced fragmentation through the role of ENISA

The introduction of the Strategy in 2013 was an attempt to overcome existing fragmentation as far as possible possible – and desirable. The 2013 Strategy gave the European Network and Information Security Agency (ENISA) authoritative status in building cyberresilience. The accompanying NIS Directive includes proposals to enhance the role of the ENISA in order to extend its coordinating role. Further, the new Basic Regulation governing ENISA provides the agency with a clear mandate to support several new areas within the realm of cybersecurity. One example given in the Strategy is that ENISA is expected to assist in the establishment and functioning of a full-scale European Union Computer Emergency Response Team (EU CERT) and a pan-EU network of CERTs to counter cyberattacks at the EU level. Moreover, 'both national entities and EU institutions may request expertise and advice from ENISA in case of a "security breach or loss of integrity with a significant impact on the operation of networks and services"'.[485]

Implementation of the EU's Strategy would also require ENISA to work on NIS-related aspects of cybercrime. For example, the Executive Director of ENISA is now part of the Programme Board of the European Cyber Crime Centre (EC3). In the words of Steve Purser, the Head of Operations of ENISA, the membership of this board is 'one of the mechanisms we use to align our work and to make sure that the fight against cybercrime is very much aligned with what ENISA is doing in terms of increasing preparedness, making sure that critical information infrastructure is protected correctly, etc.'[486] At the same time, EC3 is part of the permanent stakeholder group of ENISA. In June 2014, ENISA and EC3 signed a strategic cooperation agreement 'to facilitate closer cooperation and exchange of expertise in the fight against cybercrime'.[487] According to the press release announcing this agreement, such cooperation could include:

- The exchange of specific knowledge and expertise.
- Elaboration of general situational reports.

---

[484] Dunn Cavelty 2013b.
[485] North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2013. 'ENISA's new mandate to face cyber security challenges.' As of 12 October 2015: https://ccdcoe.org/enisas-new-mandate-face-cyber-security-challenges.html
[486] Field, Tom. 2013. 'Enisa Aims for Longer, Stronger Role: European Security Agency Extended, Strengthened by Parliament.' *Bank Info Security*, April 22. As of 12 October 2015: http://www.bankinfosecurity.com/interviews/enisa-aims-for-longer-stronger-role-i-1890
[487] ENISA. 2014. 'Fighting cybercrime: Strategic cooperation agreement signed between ENISA and Europol.' *Press Release*, June 26. As of 12 October 2015: http://www.enisa.europa.eu/media/press-releases/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol

- Reports resulting from strategic analyses and best practice.
- Strengthening capacity building through training and awareness raising, to safeguard network and information security at EU level.

Both agencies are also cooperating to organise a conference focused on CERT and law enforcement cooperation.[488]

This need for an inter-agency and cross-sectoral approach is acknowledged for broader security purposes. In April 2015, the European Commission published the European Agenda on Security (the Agenda), which states: 'It is time to deepen cooperation between these agencies (Europol and ENISA). The Commission will launch a reflection on how to maximise their contribution, through closer inter-agency cooperation, coordination with Member States, comprehensive programming, careful planning and targeting of resources.'[489]

These high-level initiatives aim to align the work of ENISA and EC3. An interviewee from EC3 reported that they 'meet regularly with ENISA' and 'work closely with them'.[490] Even though they have different focuses – law enforcement for EC3 and information security for ENISA – various initiatives have been devised to deepen their engagement. In contrast, when asked about cooperation with ENISA, an interviewee at the Member State level responded that they did not work together with ENISA and that if he came across ENISA's work, it was by 'coincidence'.[491] This indicates a lack of visibility and perhaps accessibility, which ENISA must address in order to foster greater cooperation and harmonisation.

6.2.2 Possible fragmentation due to NIS provisions regarding law enforcement

Revisions of the proposed NIS Directive may exacerbate existing fragmentation. Concerns about fragmentation relate to Article 8(3)(f) of the Commission's proposal, adopted in 2013, which initially stated that the 'cooperation network', composed of competent authorities and the Commission, must exchange information with EC3 on all relevant matters. Likewise, the European Parliament (EP) subsequently adopted a legislative resolution and 138 amendments to the proposal, which supported the clause. However, while the Council has not reached a formal stance on the proposal, its progress report indicates that it wishes to eliminate the reference to EC3 from this provision: 'As the exchange of information on criminal offences regarding attacks on information systems is covered by Directive 2013/40, there is no need for the [NIS] Directive to address this aspect.'[492] More broadly, the Council has deleted a provision that obliges the Commission to facilitate cooperation 'by means of implementing acts' and has instead called for voluntary submissions by competent authorities and CERTs to EU bodies, including Europol. Interviewees with whom the research team held discussions for this study expressed concerns that these revisions, if adopted, would effectively exclude law

[488] Interview conducted by RAND Europe with Europol.
[489] European Commission 2015, p. 4.
[490] Interview conducted by RAND Europe with Europol.
[491] Interview conducted by RAND Europe with UK National Crime Agency.
[492] Council of the European Union. 2014d. *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 - Progress report*. ST 10097 2014 INIT, May 22. As of 12 October 2015: http://data.consilium.europa.eu/doc/document/ST-10097-2014-INIT/en/pdf

enforcement authorities from the information-sharing loop at both the Member State and EU level; they will receive neither early warnings, nor incident notifications.[493]

The law enforcement community perceives this as a negative development. As the officials note, 'that translates into limiting our ability to support any actions. The information is either coming to us at a very late stage or might never come to us.'[494] A letter detailing the position of the European Cybercrime Taskforce (EUCTF) on the proposed Directive stated:

> *Failing to give law enforcement a clear role [in network and information security] would create a strong imbalance between NIS authorities – whose tasks are limited to prevention, detection and mitigation of incidents. Law enforcement authorities can play an equally vital role in the prevention of cyber incidents and also contribute to tackle one of the main causes of the problem, i.e. the growing number of criminally motivated attacks.*[495]

Law enforcement professionals interviewed argued that the amendments proposed by the Council do not recognise the role of law enforcement in overall resilience building. In written correspondence, an interviewee stated:

> *Focusing exclusively on increasing cybersecurity standards and exchanging cybersecurity information among the cybersecurity experts (CERTs, ENISA, Member State authorities) is a self-defeating strategy which ignores a crucial part of the problem. It focuses only on vulnerability mitigation.*[496]

The Council's position to remove law enforcement from the proposed cooperation framework appears inconsistent with the aims outlined in the European Agenda on Security published by the Commission in April 2015. The Agenda highlights combating cybercrime among its three priorities. The Commission writes: 'The implementation of this Directive would not only promote better cooperation between law enforcement and cybersecurity authorities, but also provide for cybersecurity capacity building of competent Member States' authorities and cross-border incident notification.'[497] Yet, as witnessed in their progress reports and verified by officials from the EC3, the Council's stance is to differentiate the NIS objectives from general law enforcement purposes. This may prevent the Commission's envisioned cooperation and exacerbate fragmentation.

6.2.3 Capability gaps and differences in priorities remain a problem

The effectiveness of the EU response is related to the differences in capability among the Member States. Various sources observe that the diversity of Member States approaches to cybersecurity – regulatory at one end of the spectrum and voluntary at the other – has led to inconsistency in capabilities. There is limited publicly available literature that gives empirical evidence to support this claim. One interviewee stated specifically: 'They vary quite significantly; there are top-end capabilities in probably half a dozen EU Member States.'[498] He described how 'the initiatives within J-CAT[499] are to bring those

[493] Interview conducted by RAND Europe with Europol.
[494] Interview conducted by RAND Europe with Europol.
[495] European Union Cybercrime Taskforce (EUCTF). 2014. *Directive on Network and Information Security*. Europol, Letter from Mr Lee Miles to Mr Datsikas (unclassified document). The Hague, April 24.
[496] Written correspondence between RAND Europe and Europol.
[497] Reeve, Tom. 2015. 'EC report: Cyber-crime demands a new approach to law enforcement.' *SC Magazine UK*, April 29. As of 12 October 2015: http://www.scmagazineuk.com/ec-report-cyber-crime-demands-a-new-approach-to-law-enforcement/article/411748/
[498] Interview conducted by RAND Europe with the UK National Crime Agency (NCA).

capabilities together. And the EMPACT level work in EUCTF is to bring the capabilities of other Member States up. There is a gap in the capabilities between the top and the bottom in terms of capacity and even understanding.'[500] Since many Member States do not make information about their full capabilities public, it is difficult to find evidence to verify this claim.

The Business Software Alliance (BSA) provides a simplified overview of Member States' capabilities based on publicly available information about (non-)existing legislation and structures in all the EU Member States. A key finding concerns capability gaps. The BSA states: 'One notable gap is the lack of systematic cooperation with non-governmental entities and public-private partnerships: a well-established framework in place for such partnerships exists in only five EU Member States. This leaves a large area untapped for effective, voluntary collaboration between governments and the private sector that owns and operates the majority of commercial critical infrastructure services in Europe.'[501] Underlying this operational gap appears a more fundamental one concerning the Member States' understanding of their vulnerabilities in the cyber domain, and their priorities among critical services and infrastructures. Addressing these differences in assessments (of vulnerabilities and priorities) may be a necessary step towards bringing their capabilities to a comparable baseline level. Indeed, one of the main aims of the NIS Directive is to address capability gaps among the Member States. The EU should therefore seek to bridge both gaps – operational capabilities and priorities among Member States – with equal and simultaneous effort.

6.2.4 NIS success requires implementation at Member State level

Given the capability gaps, and differences of opinion and priorities, the impact of the proposed NIS Directive will weigh more on Member States that have not yet institutionalised NIS as a core part of their national cybersecurity agenda. The effectiveness of the Directive in achieving its aims will depend in part on implementation at Member State level, which will then depend on the willingness of public agencies and industry to cooperate. Whether the incentives are sufficiently compelling for those countries is a fundamental question and symptomatic of the broader issue of the effectiveness of the EU cybersecurity strategy.

A report produced by FireEye, an American network security company, reported findings from polling organisations in France, Germany and the UK to determine how prepared they are for implementation of the proposed NIS Directive.[502] The report outlines a number of challenges for businesses and organisations in the three countries:[503] meeting

[499] Joint Cybercrime Action Taskforce.
[500] Interview conducted by RAND Europe with the UK National Crime Agency (NCA). EMPACT stands for European Multidisciplinary Platform Against Criminal Threats. For each EMPACT priority, Europol has specialised groups that are producing a MASP (Multi-Annual Strategic Plan), which defines the operational goals that should be achieved within the four years.
[501] Business Software Alliance (BSA). 2015. *EU Cybersecurity Dashboard: A path to a secure European cyberspace*. As of 12 October 2015: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf, p. 2.
[502] FireEye. 2015. *Mixed state of readiness for New Cybersecurity regulations in Europe – French, German and UK organisations need more clarity on compliance requirements for 2015-2017*. As of 12 October 2015: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/rpt-mixed-state-of-readiness-for-new-cybersecurity-regulations-in-europe.pdf
[503] The report surveyed '260 people working for organisations based in France, Germany and the UK each of which employ over 500 staff. Of those polled, an aggregate of 31% were IT managers and 20% IT directors, with a further 27% occupying specific IT related executive positions such as chief information officer, chief technology officer or chief security officer. The largest contingent (20%) worked in the software and computer services industry, with 11% employed in electronics, 8% engineering and 7% in financial and healthcare sectors respectively.'

implementation costs, investing in new technologies, gathering expertise and realigning existing systems to the requirements of the Directive. Among these, financing the implementation of the Directive is identified as the biggest challenge to in-house Information Technology (IT) departments, which normally bear the brunt of responsibility for overseeing NIS compliance. The FireEye report also identifies confusion among respondents about what specific security upgrades will be required. In total 42 per cent of the organisations polled claimed that they have little to no clear guidance on their obligations under the proposed Directive.[504] Without practical advice or technical standards, this is likely to widen present capability gaps. Further, implementation itself may cause fragmentation, as there is great variability in the competences of non-specialist IT departments, the size of the businesses they must deal with and the availability of intersectoral support. In the FireEye survey, only 39 per cent of organisations in France, Germany and the UK reported full readiness to comply with the Directive. Given that these Member States are considered 'advanced' in the field of NIS, it is safe to assume a much lower level of readiness among organisations in other EU Member States.

Besides, before introducing new legislation, attention must be paid to the extent to which previously introduced legislation has actually been implemented. The Agenda also emphasises the importance of implementation.[505] Here, the European Commission recognises, at least in the area of cybercrime, that 'ensuring full implementation of existing EU legislation is the first step in confronting cybercrime'.[506] The Commission therefore proposes to 'assess the level of implementation of the current legislation, consult relevant stakeholders and assess the need for further measures'.[507]

6.3 From voluntary and informal to mandatory and formal

The Commission signalled an intention to implement additional regulation to increase the participation of private sector stakeholders in the EU and at Member State level in the Strategy. The Commission remarked:

> *The players managing critical infrastructure or providing services essential to the functioning of our societies are not under appropriate obligations to adopt risk management measures and exchange information with relevant authorities.*[508]

The Commission identifies a lack of (effective) incentives for service providers to conduct periodic risk assessments and apply management measures; more importantly, the Commission attributes this lack of incentives to inadequate regulation. The new EU approach, set out in the Strategy and the NIS Directive, signals an intention to move from a voluntary and informal approach to one that is mandatory and formal.

Researchers and commentators have noted that regulation constitutes just one of many ways to enhance incentives for providers to employ appropriate risk management methods. Different perspectives are offered about the likely effectiveness of moving from an informal and voluntary to a formal and mandatory approach.

---

[504] FireEye. 2015, p. 9.
[505] European Commission 2015.
[506] European Commission 2015, p. 19.
[507] European Commission 2015, p. 19.
[508] European Commission. 2013b. *Proposal for a Directive of the European Parliament and the Council – Concerning measures to ensure a high common level of network and information security across the Union*. COM (2013) 48 Final. As of 12 October 2015: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

6.3.1 Arguments for a formal approach

The Commission noted that, according to its own records, a large number of cyberincidents in the EU go unnoticed and unreported, which is indicative of the providers' unwillingness to disclose any compromise in their systems. [509] This unwillingness to disclose vulnerabilities could be because providers do not want to damage their reputation. Reputational damage can occur when incidents take place and must be reported either to victims or to the 'competent authorities'. The Commission emphasises:

> *Information on incidents is essential for public authorities to react, take appropriate mitigating measures, and set adequate strategic priorities for NIS." The avoidance of reputational damage appears to be one of the main drivers for providers to take (additional) cybersecurity measures.*[510]

Law enforcement agencies have welcomed the mandatory reporting clause proposed by the Directive. In a letter to the EU, the head of EUCTF writes:

> *At present, in most Member States, the decision to report cyber incidents to NIS authorities as well as to the police is left to the discretion of market operators. There is clear evidence that businesses severely underreport cybercrime committed against them… The limits of this voluntary approach are increasingly being recognised.*[511]

He then concludes that mandatory reporting of cyber incidents should 'logically' ensure the transfer of information from NIS authorities to relevant law enforcement agencies, should it entail criminal elements (see Section 6.2).

6.3.2 Arguments against a formal approach

Ryan et al. note that 'moving from a voluntary to a legislative approach risks creating a "static compliance approach" that could "divert scarce security resources from areas requiring greater investment towards areas with lower priority [and] decrease Europe's collective security"'.[512]

An example of such a situation is the CERTs community. CERTs or Computer Security Incident Response Teams (CSIRTs) conventionally work through informal networks, which function on the basis of trust, and personal networks between members. These CERTs or CSIRTs are vital to generating intelligence and information sharing and can be considered to embody the notion of a 'security community'. ENISA corroborates this view of CERTs and how they operate: '[C]ooperation and collaboration takes place in a practical, informal manner between operators who have trusted relationships rather than because of any strictly formalised legal agreement.'[513] This, however, implies that the regulatory-heavy approach of the NIS Directive may be inappropriate for engendering a vibrant information security community; it may, in fact, diminish trust among CERTs and create disincentives for collaboration. Arkush et al. explain this concern:

---

[509] Libicki et al. 2015.
[510] Libicki et al. 2015.
[511] EUCTF 2014.
[512] Pearse et al. 2014.
[513] ENISA. 2011. *A Flair for Sharing – Encouraging Information Exchange Between CERTs: A Study Into the Legal and Regulatory Aspects of Information Sharing and Cross-border Collaboration of National/Governmental CERTs in Europe*. As of 12 October 2015: https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing/legal-information-sharing-1/at_download/fullReport

> *In the case of a mandatory requirement [to share information] as proposed in the NIS Directive, it is expected by the experts that the initial level of trust between participants who haven't built interpersonal relationships before might be relatively low which will impede the willingness to share information.*[514]

Lastly, this preference for an informal approach goes beyond CERTs and CSIRTs. The BSA writes:

> *As discussions around mandatory cyber incident reporting intensify, it is important to note that most European countries seem to remain reluctant to introduce such schemes, many of them favouring formal or informal cooperation with the private sector. Many fear that a mandatory requirement to notify incidents may be less effective than the exchange of information based on mutual trust and ongoing collaboration.*[515]

6.4 The scope of the NIS Directive: a recurring issue

Besides the challenges of fragmentation and opposition among some stakeholders to the compulsory character of the new EU approach, the Strategy faces a further problem with defining the appropriate scope of the proposed NIS Directive. As Young puts it, 'The scope of the NIS Directive has been controversial from the outset.'[516] While the wording of the Directive is developed further by the EP in its first reading position, the question of who does what for whom and to what extent remains deeply contested in the Council, as well as the communities concerned.

6.4.1 Who should the Directive apply to?

As to 'who', the Directive originally included the 'enablers of key internet services' – search engines, ecommerce, social networks and the like – and 'public administrations'. However, the EP made their obligations voluntary in its first reading position. The inclusion of providers of information society services prompted objections from several Member States who feared market distortions[517] and the exclusion of such providers was decisive for getting the legislative resolution passed in the EP. [518] With these amendments, the EP restricts 'who' to a 'market operator': an operator of critical infrastructure 'the disruption or destruction of which would have a significant impact in a Member States'. Although this preliminary scope has been established, it is uncertain whether it will be agreed by all stakeholders. In fact, despite the EP's decision to exclude internet enablers from the scope in March 2014, Member States have continued to discuss this issue in Council meetings and to date have not reached an agreement.[519] This is only one of various clauses on which the positions of the Commission, the EP and the Council differ.

---

[514] Arkush et al. 2013. *Feasibility study and preparatory activities for the implementation of a European Early Warning and Response System against cyber-attacks and disruptions. European Commission, DG Communications Network, Content & Technology*. As of 12 October 2015: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4438, p.23
[515] BSA 2015, p. 5.
[516] Young, Mark. 2015b. 'Update on the cybersecurity directive – over to Luxembourg?' *The National Law Review*, June 15. As of 12 October 2015: http://www.natlawreview.com/article/update-cybersecurity-directive-over-to-luxembourg
[517] Young 2015b.
[518] NATO CCDCOE. 2014. 'Developments in the European Union: NIS Directive, data protection reform, EP's response to U.S. surveillance.' As of 12 October 2015: https://ccdcoe.org/developments-european-union-nis-directive-data-protection-reform-eps-response-us-surveillance.html
[519] Young 2015b.

The discussions have been drawn out in the Council, according to Hirst, because certain Member States prefer a wider scope and are seeking to extend the Directive to include Internet Service Providers (ISPs).[520] Neutze, Director of Cyber Policy at Microsoft for the EMEA region, identifies three challenges with this overly ambitious approach of trying to protect all services equally. The first is that broad regulatory scope coupled with minimum harmonisation leads to an uneven cybersecurity patchwork for the EU. The second is the combination of a broad regulatory scope coupled with limited security resources, which leads to less security. The third is a broad regulatory scope coupled with incident reporting, which leads to data protection concerns.[521]

In response, Young describes how the Commission offered to resolve the issue of scope through delegated acts. He notes: 'This essentially would allow the Commission to define the type of companies within scope at a later date without having to go through the usual legislative procedure.' [522] Moreover, such a 'solution' does not address the fundamental disagreements that exist among the Member States. On 29 June 2015, the Council reached an understanding with the EP on the main principles of the Directive.[523] With respect to the scope, however, the press release notes: 'It was agreed that digital service platforms would be treated in a different manner from essential services. The details will be discussed at a technical level.'[524]

6.4.2 What should organisations included in the Directive do?

As mentioned above, the objective reformulated by the EP defines scope to include market operators 'the disruption or destruction of which would have a significant impact in a Member State.'

What constitutes 'significant impact' is another complicated aspect when discussing 'what' these market operators are expected to do. The obligation to report incidents arises when they might cause a 'significant impact on the security of the core services'.[525] According to the EP's amendments, whether an incident has a 'significant impact' depends on the number of users exposed, the duration of the incident and the geographical spread of its impact.[526] Nonetheless, these metrics are not strictly objective and maintaining consistency in reporting practices will therefore be challenging.

The concept of 'core services' is also inadequately defined at this point. Given the intertwined nature of systems constituting a critical infrastructure, distinguishing what is core or peripheral can be complicated. As Clemente writes, 'It is becoming harder to identify the nodes and connection points whose protection must be prioritised. The result is that in the public debate, at least, critical infrastructure sectors tend to be categorised

[520] Hirst, Nicholas. 2015. 'US Tech Firms targeted in Cybersecurity Talks.' *Politico*, May 21. As of 12 October 2015: http://www.politico.eu/article/another-path-to-cybersecurity/
[521] Neutze, Jan. 2014. 'Cybersecurity in Europe – an opportunity (about to be) missed.' *Microsoft EU Policy Blog*, October 24. As of 12 October 2015: http://blogs.microsoft.com/eupolicy/2014/10/24/cybersecurity-in-europe-an-opportunity-about-to-be-missed//
[522] Young 2015b.
[523] Council of the European Union. 2015b. 'Network and information security: breakthrough in talks with EP.' *Press Release* 538/15, 29 June. As of 12 October 2015: http://www.consilium.europa.eu/en/press/press-releases/2015/06/29-network-information-security/
[524] Council of the European Union 2015b.
[525] European Commission 2013b.
[526] Shooter, Simon. 2014b. 'European Cybersecurity Directive Moves Closer to Becoming a Reality.' *Bird & Bird*, February 17. As of 12 October 2015: http://www.twobirds.com/en/news/articles/2014/global/european-cybersecurity-directive-moves-closer-to-becoming-a-reality?utm_source=Concep%20Send&utm_medium=email&utm_campaign=MEPs%20vote%20strongly%20in%20favour%20of%20the%20proposed%20European%20Cybersecurity%20Directive_03/13/2014

very broadly, to the extent that they encompass almost every aspect of daily life. The problem, therefore, is that when everything is "critical", nothing is.'[527]

6.5 Comparison with the United States may lead to additional insights

Chapter 4 discussed in detail the United States' (US) cybercapabilities in three domains: cyberresilience, cybercrime and cyberdefence. Even though the US and the EU are not strictly comparable, experiences in the US can offer valuable insights for the EU situation.

6.5.1 Number of agencies and bodies

From the sources studied, the main lesson from the US experience is that when 'too many' agencies are involved in cybersecurity without effective deconfliction and coordination, they may offset each other's productivity. In the US, the response appears to have been to introduce a new agency or initiative whenever a weakness is identified. The introduction of the Cyber Threat Intelligence Integration Center (CTIIC) is an example of such an initiative, although its added value is difficult to assess considering – for example – the existence of the National Cybersecurity and Communications Integration Center (NCCIC). Such an approach may introduce additional complications to an already complex landscape, leading to unnecessary overlaps in mandates and conflicting interests. Even mapping US cybercapabilities proved a challenge, demonstrating how difficult it is for both outsiders and insiders to understand the various roles and responsibilities delegated in theory and in practice.

The lesson for the EU is to prevent the introduction of new but possibly redundant agencies. Unless there is a specific and demonstrable gap that requires such an introduction, the EU should focus on strengthening existing agencies and their mandates.

For instance, EC3 was introduced to address an unmet need for the EU to coordinate actions against cybercrime on a transnational setting and has proved its additional value through functioning as a centre of cooperation. During interviews, EC3 officials expressed concerns about how the current EU approach – expressed through the Strategy and the proposed NIS Directive – appears to lean towards developing new structures of information sharing while excluding existing agencies.[528]

6.5.2 Role of law enforcement in information sharing

Information sharing is a central theme that cuts across the different cybersecurity related objectives in the EU and the US. The involvement of law enforcement in information sharing in the US is self-evident, as is shown by the various proposals set forth in both houses of the US Congress. For the EU, the involvement of law enforcement in information sharing is now a contentious topic, as its involvement has seemingly been contested with regard to the proposed NIS Directive.

[527] Clemente, Dave. 2013. *Cyber Security and Global Interdependence: What is Critical?* Chatham House. As of 12 October 2015: http://158.36.137.205/hvorhenderdet/content/download/398662/1347551/file/CHJ381_Cyber_Programme_Report_WEB_3.pdf

[528] Interview conducted by RAND Europe with Europol; see also Arkush et al. 2013; EUCTF 2014.

6.5.3 Importance of implementation

Another lesson concerns implementation of security practices. Despite the emphasis on the importance of cybersecurity practices in the US, their implementation essentially depends on the will of the individual departments, which has led to challenges, extensively testified to by the Government Accountability Office (GAO). In the absence of such implementation, departments and agencies will inevitably remain more vulnerable to cyberthreats than those that voluntarily implement security practices. This connects with the discussion in this chapter on implementation and overcoming capability gaps within the Member States.

6.6 Conclusion

As indicated in the introduction, problems of operationalisation and a lack of data make it difficult to measure the effectiveness of cybersecurity in the EU. Cybersecurity is very much in flux at the EU level. Efforts made during the last few years have tried to tackle some previously identified challenges. This chapter has reviewed possible barriers to effectiveness and provides a critique of the likely effectiveness of proposed reforms.

The overarching challenge is fragmentation: there is a need to improve coordination and cooperation. Some initiatives, namely agreements between ENISA and EC3, have aimed to allow for more cross-agency or cross-mandate cooperation. Yet positions on the proposed NIS Directive with regard to the role of law enforcement are varied. The discussions in the Council indicate that law enforcement may be largely excluded from the information sharing provisions, which may inadvertently enhance fragmentation. The second major challenge concerns the nature of the EU approach, which is essentially divided between an informal and voluntary approach as opposed to a formal and involuntary approach. Arguments have been made in favour of both approaches in discussions about the proposed NIS Directive. The third challenge is contention about the scope of the various regulations.

As a result, while there is pressure to agree on a NIS Directive, fundamental questions remain in terms of approach and scope. As Ryan et al. observe, 'The lack of consensus could undermine the overall effectiveness of national strategies, the consistent application of the Directive across Member States and any coordinated attempts to deal with cyberthreats.'[529]

With these challenges in mind, Dunn Cavelty emphasises building cyberresilience and encourages the policy community to go beyond rhetoric: 'While resilience is recognized as a crucial element of cyber-security, there also are relatively little specific efforts to operationalize and implement it.'[530] Dunn Cavelty also notes that the EU is not alone in this regard; a lack of implementation is one of the core issues in resilience approaches across the globe: 'If resilience is to be applied in a targeted and gainful manner, four issues must be dealt with in practical terms: Political actors need clarity about the nature of the desired resilience; the goals of resilience policy; the concrete instruments to be used in fostering resilience; and the question of how to measure current and future resilience levels.'[531] She continues: 'If Europe wants to be or rather become cyber-resilient, it must look at these questions sooner rather than later and in much more detail.'[532]

[529] Pearse et al. 2014.
[530] Dunn Cavelty 2013b, p. 6.
[531] Dunn Cavelty 2013b, p. 6.
[532] Dunn Cavelty 2013b, p. 6.

7 CONCLUSIONS AND POLICY OPTIONS

This study had five objectives:

1. To identify key cyberthreats faced by the EU and the challenges associated with their identification.
2. To identify the main cybersecurity capabilities in the EU.
3. To identify the main cybersecurity capabilities in the United States (US).
4. To assess the current state of transnational cooperation.
5. To explore perceptions as to the effectiveness of the current EU response.

To accomplish these aims, this study primarily provided descriptive overviews based on document reviews and supplemented with a limited number of interviews with officials from the United Kingdom (UK) National Crime Agency (NCA), Europol's European Cyber Crime Centre (EC3), Eurojust, the United States (US) Federal Bureau of Investigation (FBI) and the Icelandic police. The two case studies on transnational cooperation were Operation Source and Operation BlackShades.

7.1 Defining cybersecurity

Any study on cybersecurity must address the challenge of the definition, or rather the absence of a standard definition, of the term. Cybersecurity is an ambiguous term used to describe a complex and challenging area of public policy. The ambiguity stems in part from the observation that the more technically minded community has been using the term 'information security' for years; the arrival of the term cybersecurity largely came about as the topic moved more into the realm of public policy and national security. This has changed the dynamic of the stakeholders involved and has introduced competing – and at times conflicting – interests, which enhances the complexity of the challenges already faced by those present in the cybersecurity landscape. The observation that cybersecurity means different things to different people has consequences. The way in which the issue is framed influences what constitutes a threat as well as what measures are needed and justified. Moving forward in the area of cybersecurity requires recognition of this observation.

7.2 Mapping cybersecurity threats

Understanding the threat landscape provides stakeholders with information about how they could be attacked and therefore what defensive measures they need to take to protect themselves. This study identified a number of challenges in relation to undertaking threat assessments and developing an overview of the threat landscape:

- There is no standard approach to categorising threats.
- The empirical or evidential basis for publicly available threat assessments is often unclear and assessments frequently refer to other assessments (rather than referring to original sources).

This study has aimed to analyse the different aspects of threat assessments and to move towards a more robust classification framework that might be used by others in future analysis. Through a review of six threat assessments, this study classified three types of threat actors: states, profit-driven cybercriminals and hacktivists or extremists. Focusing on technological threat tools, the study also described malware and its variants. Five

types of threat were identified: unauthorised access, disclosure, modification of information, destruction and denial of service.

Bearing in mind the limitations of threat assessments, the study identified the main threats as states and profit-driven criminals. These two categories require different responses since different cybersecurity capabilities are legally and operationally equipped to respond to them. From a capabilities perspective, this is a crucial observation. Cybercriminals mainly fall within the remit of law enforcement, whereas actions taken by states become an issue of national security. This relates to the discussion about how cybersecurity is defined and what implications this has on policy ownership.

7.3 Cybersecurity capabilities in the EU

The EU Cyber Security Strategy published in 2013, along with the proposal for a Network and Information Security (NIS) Directive, set the stage for an overarching approach to cybersecurity in the EU. The Strategy sets out five objectives and in this study the team focused on the first three in order to describe cybercapabilities: cybercrime, cyberresilience and cyberdefence.

This study provided an overview of the institutional structures in place in the EU and described the role the different entities currently play according to their mandates. Overall, there are three main institutional players: the European Network and Information Security Agency (ENISA); the European Cyber Crime Centre (EC3); and the European Defence Agency (EDA). These have individual mandates for different aspects of the cybercapability in the EU. They are supported by a number of additional players, including Computer Emergency Response Teams (CERTs).

ENISA plays a leading role in the area of cyberresilience. According to its mandate, ENISA has the authority to force Member States to take necessary actions, as its advice forms the core of the Commission's harmonisation strategy.

In the area of cybercrime, EC3 along with Eurojust plays a pivotal role in facilitating and coordinating the fight against cybercrime. Through strategic analysis, EC3 offers comprehensive advice on emerging trends and methods of criminal activity to policymakers. Where identified threats are of high order and magnitude, the Joint Cybercrime Action Taskforce (J-CAT) brings in the expertise of various liaising authorities beyond the EU to coordinate an international response.

In the area of cyberdefence, where the role of the EU is least pronounced, the EDA leads capability development.

7.4 Cybersecurity capabilities in the US

The landscape in the US is more diverse and arguably more complex to map in comparison to the EU. The US maintains a lengthy history with respect to cybersecurity policy, dating back to 1998 when the US government began its efforts to address cyberspace-related risks. In the years since, the question of effectiveness has been a focal point of discussion. Within each of the three objectives used to categorise capabilities (cybercrime, cyberresilience and cyberdefence), various players have a role to play and often have to engage in the challenging exercise of determining who has to do what, when and how.

In the area of cyberresilience, the US Department of Homeland Security (DHS) has a formal leadership role and maintains various responsibilities, including securing Federal Civilian Government Networks, protecting critical infrastructure and responding to

cyberthreats. Questions have been raised about the enforcement power of DHS, in particular with regard to the securing of Federal Civilian Government Networks. Compliance with the Federal Information Security Management Act (FISMA) is voluntary, although DHS does have the authority to issue binding operational directives. Incidents at federal government level, however, such as the recent intrusion at the Office of Personnel and Management (OPM), have rekindled questions about effectiveness, especially as departments and agencies have lagged behind in implementation of security practices.

In the area of cybercrime, there is no lead investigative agency. Capability in this area is dispersed across a number of agencies, namely the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). Overlaps in mandates have led to challenges but coordination efforts are in place as a means to enhance cooperation. The National Cyber Investigative Joint Task Force (NCIJTF) brings together 19 US agencies from the law enforcement and intelligence community to coordinate investigations in the cyber arena.

In the area of cyberdefence, the Department of Defense (DoD) leads the way. The DoD contains the US Cyber Command (USCYBERCOM), which has been fully operational since 2010. Several documents have been published in the area of cyberdefence, with the most recent strategy published in April 2015. In that strategy, the DoD has become more open about its offensive capabilities and has also been more forthcoming in naming its adversaries. Deterrence is also a crucial part of the strategy.

Cutting across all these areas is the topic of information sharing, where many initiatives have been introduced by both the House and the Senate. Proposed initiatives have encountered challenges from a privacy and civil liberties perspective. Even though information sharing is recognised as an integral part of cybersecurity activities, experts also indicate that its importance should not be overestimated and should not overshadow other security practices essential to improving the overall level of cybersecurity.

7.5 Transnational cooperation

The importance of transnational cooperation has been recognised both inside and outside the EU. There are various initiatives at both the strategic and operational level, to enhance cooperation and improve efforts in the area of cybersecurity in general and cybercrime in particular.

At the operational level there have been examples where law enforcement as well as judicial entities in different jurisdictions have worked together to disrupt cybercrime operations. In this study two case studies have been used to showcase who is involved, how such cooperative engagements function in practice and how different stakeholders interact with one another. The learning from these case studies appears to be that successful cooperation comes about when there is a shared interest and an ability to communicate quickly with partners across the globe.

Through interviews with experts and a review of the available literature, this study has identified challenges to transnational cooperation. One challenge related to the Mutual Legal Assistance Treaty (MLAT); interviewees indicated that under this process access to information needed for cybercrime operations could be slow to obtain. Interviewees also noted challenges stemming from the ruling of the European Court of Justice (ECJ) in relation to data retention, which can reduce the availability of information needed in cybercrime operations. The different interpretations of the Member States with regard to

the ruling have left behind a fragmented landscape, leading to law enforcement challenges.

7.6 Effectiveness of the EU response

Through creation of an overarching Cyber Security Strategy (2013), the EU has aimed to reduce fragmentation and increase coordination and harmonisation in the area of cybersecurity. Capabilities at the EU level are still in development and challenges identified before the Strategy still seem to be present; this is supported by findings from the literature and our interviews. Although some signs of improvement are on the horizon, many concerns remain:

- Fragmentation, while lessening, is potentially exacerbated through the exclusion of law enforcement from key provisions relating to information sharing in the proposed NIS Directive.
- Capability gaps and differences of priorities with regard to cybersecurity between Member States remain a problem, may hamper the effectiveness of the EU response and might have knock-on effects in terms of whether all Member States are able to implement the provisions of the NIS Directive consistently, when it is agreed. The success of the Directive will rest on implementation by all Member States.
- The Strategy and the draft NIS Directive propose a change in the regulatory environment in relation to cybersecurity, from the current system in which the involvement and cooperation of key actors are largely not legally mandated, to a system that is characterised by a mandatory and formal approach. This proposed change is both welcomed and criticised.
- The European Commission, the Council and the European Parliament disagree on the appropriate scope of the proposed NIS Directive, in terms of the actors and entities to whom it should apply. The scope of the Directive could have important consequences for the effectiveness of the EU response to cybersecurity.

This study has identified some possible lessons regarding the effectiveness of the response to cybersecurity from the US. Researchers studying the US system highlight that the introduction of new players as well as the involvement of too many institutions may further complicate an already complex landscape. With over 62 federal offices involved in the area of cybersecurity (according to one account), overlaps between mandates are almost guaranteed and have indeed been identified by US authorities. When incidents do occur, the allocation of responsibility becomes a focal point. This suggests that the EU might want to be cautious in creating new bodies or creating overlapping mandates between existing bodies.

Another lesson to be learned from the US situation is the necessity for departments and agencies to implement recommendations and best practices set forth by knowledge and expertise centres. Implementation is also key in the EU, where Member States maintain different opinions on, for example, what the scope of the NIS Directive should be. Given the particular challenges the EU faces in regulating its cyber domain, the ongoing discussion about the NIS Directive should reflect further on the feasibility of the suggested policy as well as its probability of success.

7.7 Policy options

Based on the findings of this study, the research team highlights a number of possible policy options for consideration by the European Parliament (EP).

1. **Encourage ENISA, EC3 and others involved in European cyberthreat assessments to investigate further harmonisation of threat assessments, which can effectively incorporate information from Member States and other EU agencies and provide clearer indications of the evidence base for the assessment.** This recommendation follows from the findings of the review of threat assessments undertaken for this study. It was found that the evidence underlying the identified threats was not clear, nor was the approach to identifying and prioritising threats. Threat assessment reports ought to be more transparent about their methodological approach and should include a comprehensive bibliography of sources as well as an improved taxonomy of threats. As a lead organisation in cybersecurity in the EU, ENISA could improve its threat landscape to provide a clearer delineation between threats, threat tools and vulnerabilities.
2. **Make use of existing structures as much as possible.** One of the concerns identified by the study team, from a review of the existing literature and interviews with experts, is the tendency within the EU to develop new structures in addition to existing initiatives and agencies. Through EC3, Eurojust and ENISA, the EU already has a number of agencies in the area of cybersecurity and it would be beneficial to use these where appropriate to carry out the objectives of the Strategy. The main benefit of making use of existing structures is the avoidance of duplication of mandates or other potential overlaps leading to lack of clarity and inefficiency. The situation in the US is a helpful example in this regard, since the US experiences ongoing challenges due to its layered approach.
3. **Consider reinserting law enforcement in the Network and Information Security (NIS) Directive.** The attempt to overcome fragmentation at the EU level could be hampered by the exclusion of law enforcement from information sharing provisions in the proposed NIS Directive. Even though the Council states that information sharing with respect to law enforcement is taken care of in Directive 2013/40/EU, one of the main aims of the proposed NIS Directive is to overcome fragmentation. The view of those in favour of including law enforcement is that law enforcement forms an integral part of the fight against cybercrime specifically, and could help cybersecurity generally, as its actions also assist cyberresilience. As a result, law enforcement needs to remain in the NIS Directive to facilitate the reduction of fragmentation.
4. **Ensure Europol has speedy and more direct access to information from the private sector**. Cybercrime occurs at a rapid pace and is inherently transnational in nature. Speedy access to relevant information from the private sector is essential for action against cybercrime. The potential for such access to be hindered by having to go through the Member States may lead to the reduced effectiveness of Europol operations especially as they cooperate with partners at the transnational level. For the proposed regulation on Europol, the EU institutions should therefore ensure that, while guaranteeing protection for the privacy and civil liberties of citizens, Europol is able to access legally valuable information held by the private sector for the purposes of cybercrime investigations.

5. **Assess what capability gaps actually exist between the Member States and measure progress.** Empirical evidence to indicate the different levels of cybercapability across Member States is currently absent from the public domain. To improve the situation and to develop a better understanding of these gaps, a more robust and empirically based assessment could be undertaken to identify areas of improvement and make these more explicit. This would allow progress to be measured more accurately against a baseline and more advanced Member States might be able to assist those Member States that are developing their capabilities. ENISA and the EDA could be well placed to play a role in identifying clearly the capability gaps of Member States.

GLOSSARY OF TERMS

Advanced Encryption Standard (AES) A block cipher standard developed by the US National Institute of Standards and Technology (NIST) that replaced the Data Encryption Standard (DES). [533] The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.[534]

Advanced Persistent Threats (APT) APTs are covered attacks stealing vulnerable data. In specific terms, 'advanced' means it gets through the existing defense system and 'persistent' makes clear that it succeeds in hiding from your existing level of detection. [535]

Botnets A network of remotely controlled systems used to coordinate attacks such as distribute malware, spam, and phishing scams. Bots (short for robots) are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.[536]

DDoS attack A type of attack used to prevent legitimate users from accessing online services or resources. Typically, a network is brought down by flooding it with traffic so legitimate traffic cannot pass through.[537]

Domain generating algorithm (DGA) An algorithm within a malware product that creates a list of new command-and-control servers as part of a cyclical update routine.[538]

Domain name system (DNS) A computing system which distributes 'easy-to-remember' names instead of IP addresses, by trainslating domain names to IP addresses and back. [539]

---

[533] McAfee. n.d. 'Glossary of Technical Terms.' As of 12 October 2015: https://kc.mcafee.com/corporate/index?page=glossary

[534] National Institute of Standards and Technology (NIST). 2001. *Announcing the Advanced Encryption Standard*. FIPS PUB 197, November 26. As of 12 October 2015: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[535] McAfee. 2011. *Combating Advanced Persistent Threats – How to prevent, detect, and remediate APTs*. As of 12 October 2015: http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf

[536] McAfee. n.d.

[537] Ablon, Lillian, Martin C. Libicki & Andrea A. Golay. 2014. *Markets for Cybercrime Tools and Stolen Data - Hacker's Bazaar*. Santa Monica, Calif.: RAND Corporation. As of 12 October 2015: http://www.rand.org/pubs/research_reports/RR610.html

[538] InfoSec Institute. 2014. 'Domain Generation Algorithm (DGA).' *General Security*, 23 June. As of 12 October 2015: http://resources.infosecinstitute.com/domain-generation-algorithm-dga/

Drive-by attacks Drive-by attacks are attacks in which a system is being infected by visiting a website that is running malicious code.[540] These types of attacks usually work in conjunction with an exploit kit that is deployed on a so called 'landing page' to which the visitors are being redirected.[541]

Exploits An exploit take advantage of weaknesses or "vulnerabilities" in common software.[542]

Exploit Kit An exploit kit is a fully automated toolkit that is systematically searching for unpatched vulnerabilities for the purpose of injecting malicious content.[543] As of 2015, there are around 70 different exploit kits operating in the wild taking advantage of hundreds of vulnerabilities.[544] The most popular kits are: Sweet Orange, Angler, and Magnitude.[545]

File-less Malware File-less malware is malware that does not exist as a file on an infected system.[546] Instead it resides in the system memory, such as the Windows registry, to bypass detection.[547] Its utilization of native Windows tools, such as Powershell and Microsoft CryptoAPI, makes it very difficult to distinguish from legitimate user activity.[548]

Malware A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.[549]

---

[539] Chandramouli, Ramaswamy & Rose Scott. 2013. *Secure Domain Name System (DNS) Deployment Guide*. NIST Special Publication 800-81-2. As of 12 October 2015: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf
[540] Ragan, Steve. 2013. 'NBC cleans up site after citadel compromise.' *Securityweek.com*, 22 February. As of 12 October 2015: http://www.securityweek.com/nbc-cleans-site-after-citadel-compromise
[541] Zorabedian, John. 2014. 'How malware works: Anatomy of a drive-by download web attack (infographic).' *Sophos*, 26 March. As of 12 October 2015: https://blogs.sophos.com/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/
[542] Microsoft. n.d. 'The Exploit Malware Family.' *Microsoft Malware Protection Center*. As of 12 October 2015: http://www.microsoft.com/security/portal/mmpc/threat/exploits.aspx
[543] Chen, Joseph C. & Brooks Li. 2015. *Evolution of Exploit Kits – Exploring past trends and current improvements*. TrendMicro Research Paper. As of 12 October 2015: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf, p. 1
[544] Chen & Li 2015, p. Introduction.
[545] Chen & Li 2015, p. 3.
[546] O'Murchu, Liam & Fred P. Gutierrez. 2015. *The evolution of the fileless click-fraud malware Poweliks*. Symantec Security Response. As of 12 October 2015: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/evolution-of-poweliks.pdf
[547] O'Murchu & Gutierrez 2015, p. 11.
[548] Maude, James. 2015. 'File less fears.' *Avecto Blog*, 1 May. As of 12 October 2015: https://blog.avecto.com/2015/05/file-less-fears/
[549] Kissel, Richard. 2013. *Glossary of Key Information Security Terms*. National Institute of Standards and Technology (NIST), NISTIR 7298 Revision 2. As of 12 October 2015: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Malvertisement An infected online advertisement hosted on malicious-, legitimate sites and social networks.[550] A user can get infected by simply visiting a site,[551] or clicking on the malvertisement, which will either directly install malware or redirect to an exploit kit.[552]

Patches A type of programming code that is used to repair an identified software bug or vulnerability.[553]

Phishing A scamming technique that uses spam or pop-up messages to deceive people into disclosing credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. Internet scammers use email bait to "phish" for passwords and financial data from Internet users.[554]

Point of Sale malware (PoS) Malicious software expressly written to steal customer payment data -- especially credit card data -- from retail checkout systems. Criminals often purchase POS malware to steal customer data from a retail organization with the intention of selling the data rather than using it directly.[555] Point-of-sale malware is highly customized malicious software written to identify, aggregate and exfiltrate cardholder data.[556]

Polymorphic downloader A downloader is a type of malware specifically created for the purpose of downloading other malware, including password stealers, rootkits, fake antivirus, and ransomware.[557] Polymorphic describes the ability of a malware to change parts of itself to avoid detection by security software.[558]

---

[550] TrendMicro. n.d. 'Malvertisement definition.' As of 2 October, 2015: http://www.trendmicro.com/vinfo/us/security/definition/Malvertisement
[551] MicroData. 2015. 'Malvertisement Alert! Firefox and IE Users affected.' *MicroData Blog*, 4 February. As of 12 October 2015: http://blog.microdata.com/malvertisement-alert-firefox-and-ie-users-affected/
[552] Segura, Jerome. 2015. 'Large Malvertising Campaign goes (almost) undetected.' *Malwarebytes.com*, 14 September. As of 12 October 2015: https://blog.malwarebytes.org/malvertising-2/2015/09/large-malvertising-campaign-goes-almost-undetected/
[553] Norton. n.d. 'Glossary.' As of 12 October 2015: http://us.norton.com/security_response/glossary/define.jsp?letter=p&word=patch
[554] McAfee. n.d.
[555] Rouse, Margaret & Matthew Haugh. 2015. 'POS malware (point-of-sale malware).' *WhatIS.com*, January. As of 12 October 2015: http://whatis.techtarget.com/definition/POS-malware-point-of-sale-malware
[556] Trustwave. 2014. *White Paper: Combatting Point of Sale Malware*. As of 12 October 2015: http://www2.trustwave.com/rs/trustwave/images/Special_Report_Combatting_Point_of_Sale_Malware.pdf
[557] Intel Security. 2014. *Catch me if you can - Antics of a polymorphic Botnet*. As of 12 October 2015: http://www.mcafee.com/us/resources/misc/infographic-catch-me-if-you-can.pdf
[558] Microsoft. n.d. 'Malware Protection Center – Glossary.' As of 12 October 2015: https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx

RAM scraping malware	A type of malware that examines the random-access memory (RAM) to search for sensitive data, which are not available through other processes.[559]
Ransomware	A type of malware that prevents or limits users from accessing their system. Ransomware forces its victims to pay a ransom through certain online payment methods in order to grant access to their systems or to get their data back. Some ransomware (Cryptolocker) encrypts files. Other ransomware uses TOR to hide command-and-control communications (CTB Locker).[560]
Rootkit	Software that hides itself or other objects, such as files, processes and registry keys, from standard diagnostic, administrative and security software. [561]
Sinkholing	A technique that allows for the disruption of malicious networks by injecting crafted information in the list of peers of every bot. This modifies the structure of the network, turning it into a centralised network. The injected node can be controlled by the defender or can be inexistent, making all the bots point to a black hole.[562]
Trojans (including banking Trojans)	Trojans, or Trojan horses, are files that masquerade as desirable programs but are in fact malicious. Trojan horses contain malicious code that causes loss or theft of data. For a Trojan horse to spread, users must invite these programs onto their computer, for example, by opening an email attachment. A very important distinction from true viruses is that Trojans do not replicate themselves.[563]
Watering Hole	In a Watering Hole scenario, threat actors infect a carefully selected website by inserting an exploit resulting in malware infection.[564]

[559] Rouse, Margaret. n.d. 'Memory-scraping Malware.' As of 12 October 2015: http://searchsecurity.techtarget.com/definition/memory-scraping-malware
[560] TrendMicro. n.d. 'Definition: Ransomware.' As of 12 October 2015: http://www.trendmicro.com.au/vinfo/au/security/definition/ransomware
[561] Butler, Jamie et al. 2013. 'R_: The Exponential Growth of Rootkit Techniques.' As of 12 October 2015: http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Butler.pdf
[562] Casenova, Matteo & Armando Miraglia. 2014. *Botnet over Tor: The Illusion of Hiding*. https://ccdcoe.org/cycon/2014/proceedings/d3r2s3_casenove.pdf
[563] Norton. n.d. 'Glossary.' As of 12 October 2015: http://us.norton.com/security_response/glossary/define.jsp?letter=t&word=trojan-horse
[564] TrendMicro. n.d. 'Threat Encyclopedia – Watering Hole 101.' As of 12 October 2015: http://www.trendmicro.com.au/vinfo/au/threat-encyclopedia/web-attack/137/watering-hole-101

Web application attacks

A web application attack consists of feeding vulnerable servers and/or mobile apps with malicious input or unexpected sequences of events. The objective is to inject malicious code, alter site content or breach information.[565]

Web-based attacks

A web-based attack covers all available techniques regarding redirection of web browsers to malicious websites where further malware infections may take place. Web-based attacks are facilitated by the fact that malicious URLs are easy to implement and seen as the most common vulnerability (easy to exploit and redirect to malicious sites).[566]

Worms

A worm is a type of malware that is a self-replicating, self-propagatin, self-contained program that uses networking mechanisms to spread itself.[567]

Zero-day exploit

A zero-day exploit is defined as a software or hardware vulnerability that has been exploited by an attacker and of whose existence the general information security community remains ignorant.[568] As a result, no patch or fix is available to defend against it.[569]

[565] ENISA. 2015a. *ENISA Threat Landscape 2014*. As of 12 October 2015: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014
[566] ENISA 2015a.
[567] Kissel 2013.
[568] Bu, Zheng. 2014. 'Zero-day attacks are not the same as zero-day vulnerabilities.' *Fireye Blog*, 24 April. As of 12 October 2015: https://www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html
[569] Bu 2014.

ANNEX: METHODOLOGY

For Chapter two, the project team identified the most authoritative threat assessments based on its experience and awareness of the threat assessment landscape. The study team also used the overview provided by the meta-analysis of Gehem et al.

For the chapter on EU cybersecurity capabilities, the project team identified the most relevant agencies based on those identified in the EU Strategy. For the description of their role and accompanying information, the project team searched for their official documents as well as the information provided on their website, and other official EU documentation describing their mandate or role. For the overview of the NIS Directive, the analysis was supplemented by commentary from other online sources.

For the chapter on US cybersecurity capabilities, the project team searched on Google using terms such as 'cybersecurity United States', 'cybersecurity federal government' and also specific agencies and departments such as the Department of Homeland Security (DHS), Department of Defense (DoD), Federal Bureau of Investigation (FBI), etc. Targeted searches were also carried out on the website of the Government Accountability Office (GAO), which is recognised as an authoritative source on the subjects related to the federal government in the area of cybersecurity.

The chapter on effectiveness benefited from insights provided by interviews with the European Cyber Crime Centre (EC3) as well as Google searches using keyword combinations of EU, cybersecurity and effectiveness. Sources used include commentary pieces either from media outlets or from law offices reflecting on the developments surrounding the proposed NIS Directive in particular.

For the transnational cooperation part of the study, the study team carried out two case studies based on desk research and publicly available documentation. These were supplemented by interviews with officials from EC3, the FBI, Eurojust, the National Crime Agency (NCA) and the Icelandic police. These interviews were used specifically to identify remaining challenges and recommendations for improvement. For the interviews, a more informal approach was used to engage in a discussion with respondents about challenges, good practice and recommendations for improvement in transnational cooperation.

REFERENCES

- Allan, Darren. 2015. 'Intel spearheaded international effort to down Beebone botnet.' *ITProPortal.com*, April 10. As of 12 October 2015: http://www.itproportal.com/2015/04/10/intel-spearheaded-international-effort-beebone-botnet/

- Ablon, Lillian, Martin C. Libicki & Andrea A. Golay. 2014. *Markets for Cybercrime Tools and Stolen Data - Hacker's Bazaar*. Santa Monica, Calif.: RAND Corporation. As of 12 October 2015: http://www.rand.org/pubs/research_reports/RR610.html

- Anderson, Ross et al. 2012. 'Measuring the Cost of Cybercrime.' In the *Workshop on the Economics of Information Security*. As of 12 October 2015: http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

- Archick, Kristin. 2002. *Cybercrime: The Council of Europe Convention*. Congressional Research Service. As of 12 October 2015: http://digital.library.unt.edu/ark:/67531/metacrs2394/m1/1/high_res_d/RS21208_2002Apr26.pdf

- Arena, Mark. 2015. 'Cyber threat intelligence: Comparing the incident-centric and actor-centric approaches.' *Intel471*, June 15. As of 12 October 2015: http://www.intel471.com/blog-incident-centric-versus-actor-centric.html

- Arkush et al. 2013. *Feasibility study and preparatory activities for the implementation of a European Early Warning and Response System against cyber-attacks and disruptions*. European Commission, DG Communications Network, Content & Technology. As of 12 October 2015: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4438

- Australian Cyber Security Centre (ACSC). *2015. 2015 Threat Report*. Canberra: Australian Government. As of 2 September 2014: https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

- Barwick, Hamish. 2015. 'Cybercrime-as-a-service on the rise says government report.' *ComputerWorld*, July 29. As of 12 October 2015: http://www.computerworld.com.au/article/580687/cybercrime-as-a-service-rise-says-government-report/

- BBC. 2014. 'BlackShades: Arrests in computer malware probe.' *BBC*, May 19. As of 12 October 2015: http://www.bbc.com/news/uk-27471218

- Bennett, Cory. 2015. 'Senators unveil new Homeland Security cyber bill.' *The Hill*, July 22. As of 12 October 2015: http://thehill.com/policy/cybersecurity/248775-senators-set-to-unveil-new-dhs-cyber-bill

- Bowcott, Owen. 2015. 'High court rules data retention and surveillance legislation unlawful.' *The Guardian*, 17 July. As of 12 October 2015: http://www.theguardian.com/world/2015/jul/17/data-retention-and-surveillance-legislation-ruled-unlawful

- Brantly, Aaron F. 2014. 'The Cyber Losers.' *Democracy and Security* 10(2): 132-155

- Brauch, Hans Gunter. 2011. 'Concepts of security threats, challenges, vulnerabilities, and risks.' In: Brauch et al. 2011. *Coping with Global Environmental Change, Disasters, and Security.* Berlin: Springer-Verlag.

- Broeders, Dennis. 2015. *The Public Core of the Internet: An International Agenda for Internet Governance*. WRR Scientific Council for Government Policy, Policy Brief 2. As of 12 October 2015: http://www.wrr.nl/fileadmin/en/publicaties/PDF-WRR-Policy_Briefs/WRR_Policy_Brief__2015__The_Public_Core_of_the_Internet.pdf

- Bu, Zheng. 2014. 'Zero-day attacks are not the same as zero-day vulnerabilities.' *Fireye Blog*, 24 April. As of 12 October 2015: https://www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html

- Bundesamt für Sicherheit in der Informationstechnik (BSI). 2014. *The State of IT Security in Germany 2014.* Bonn: BSI. As of 12 October 2015: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile

- Bundeskriminalamt (BKA). 2014. 'EUROPOL-Operation "BlackShades": 19 Tatverdächtige in Österreich ausgeforscht.' As of 12 October 2015: http://www.bmi.gv.at/cms/BK/presse/files/2052014_BlackShades.pdf

- Burr, Richard. 2015. *Report together with additional views – Cybersecurity Information Sharing Act 2015*. Congress.gov, 15 April. As of 12 October 2015: https://www.congress.gov/114/crpt/srpt32/CRPT-114srpt32.pdf

- Business Software Alliance (BSA). 2015. *EU Cybersecurity Dashboard: A path to a secure European cyberspace*. As of 12 October 2015: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.

- Butler, Jamie et al. 2013. 'R_: The Exponential Growth of Rootkit Techniques.' As of 12 October 2015: http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Butler.pdf

- Carman, Ashley. 2015. 'White House criticizes bill clarifying Cyber Threat Intelligence Integration Center missions.' *SC Magazine*, June 22. As of 12 October 2015: http://www.scmagazine.com/obama-administration-issues-statement-on-intelligence/article/422126/

- Casenova, Matteo & Armando Miraglia. 2014. *Botnet over Tor: The Illusion of Hiding*. https://ccdcoe.org/cycon/2014/proceedings/d3r2s3_casenove.pdf

- CERT-EU. 2013. 'RFC 2350.' As of 12 October 2015: http://cert.europa.eu/static/RFC2350/RFC2350.pdf

- Chandramouli, Ramaswamy & Rose Scott. 2013. *Secure Domain Name System (DNS) Deployment Guide*. NIST Special Publication 800-81-2. As of 12 October 2015: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf

- Chen, Joseph C. & Brooks Li. 2015. *Evolution of Exploit Kits – Exploring past trends and current improvements*. TrendMicro Research Paper. As of 12 October 2015: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf

- Choucri, Nazli, Gihan Daw Elbait & Stuart Madnick. 2012. *What is Cybersecurity? Explorations in Automated Knowledge Generation.* As of 12 October 2015: http://ecir.mit.edu/images/stories/Madnick%20et%20al%20Comparison%20Paper%20for%20ECIR%20workshop%20-%20Fig%201%20also%20FIXED%20v2.pdf

- Clapper, James R. 2015. *Worldwide Threat Assessment of the US Intelligence Community – Statement for the Record*. Senate Armed Services Committee, February 26. As of 12 October 2015: http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-26-15.pdf

- Clemente, Dave. 2013. *Cyber Security and Global Interdependence: What is Critical?* Chatham House. As of 12 October 2015: http://158.36.137.205/hvorhenderdet/content/download/398662/1347551/file/CHJ381_Cyber_Programme_Report_WEB_3.pdf

- CNN Money. 2015. 'Adult dating site hack exposes sexual secrets of millions.' *CNN*, May 22. As of 12 October 2015: http://money.cnn.com/2015/05/22/technology/adult-friendfinder-hacked/

- Cornish, Paul, Rex Hughes & David Livingstone. 2009. *Cyberspace and the National Security of the UK.* Chatham House. As of 12 October 2015: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r0309cyberspace.pdf

- Corrin, Amber. 2012. 'DHS feels growing pains in cybersecurity role.' *FCW*, October 17. As of 12 October 2015: http://fcw.com/articles/2012/10/17/dhs-cybersecurity.aspx

- Corrin, Amber. 2015. 'Does cyber breach illuminate a $3B DHS failure?' *C4ISR & Networks*, July 13 As of 12 October 2015: http://www.c4isrnet.com/story/military-tech/omr/opm-cyber-report/2015/06/05/opm-breach-einstein-dhs/28556635/

- Council of Europe. 2001. 'Convention on Cybercrime (Budapest Convention).' As of 12 October 2015: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

- Council of Europe. 2015a. 'Convention on Cybercrime: Status as of 24/8/2015.' As of 12 October 2015: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

- Council of Europe. 2015b. *Assessment report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime*. Cyber Crime Convention Committee, June 21. As of 12 October 2015: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b

- Council of the European Union. n.d. 'Strategic guidelines for justice and home affairs.' As of 12 October 2015: http://www.consilium.europa.eu/en/policies/strategic-guidelines-jha/

- Council of the European Union. 2002. *Setting up Eurojust with a view to reinforcing the fight against serious crime*. Council Decision 2002/187/JHA, 28 February. As of 12 October 2015: http://eurojust.europa.eu/doclibrary/Eurojust-framework/ejdecision/Eurojust%20Decision%20(Council%20Decision%202002-187-JHA)/Eurojust-Council-Decision-2002-187-JHA-EN.pdf

- Council of the European Union. 2003. *Amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime*. Council Decision 2003/659/JHA, 18 June. As of 12 October 2015: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejdecision/2003%20Amendment%20to%20Eurojust%20Decision%20(Council%20Decision%202003-659-JHA)/Eurojust-Council-Decision-2003-659-JHA-EN.pdf

- Council of the European Union. 2009. *On the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime*. Council Decision 2009/426/JHA, 16 December. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009D0426

- Council of the European Union. 2011. *Defining the statute, seat and operational rules of the European Defence Agency and repealing Joint Action 2004/551/CFSP*. Council Decision 2011/411/CFSP, 12 July. As of 12 October 2015: https://www.eda.europa.eu/docs/documents/eda_council_decision.pdf

- Council of the European Union. 2014a. *Outcome of Proceedings – EU Cyber Defence Policy Framework*. As of 12 October 2015: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

- Council of the European Union. 2014b. *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA (First reading)*. As of 12 October 2015:

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010033%202014%20INIT

- Council of the European Union. 2014c. *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 - Preparations for the 1st informal exploratory trilogue*. ST 14076 2014 INIT, October 8. As of 12 October 2015: http://data.consilium.europa.eu/doc/document/ST-14076-2014-INIT/en/pdf

- Council of the European Union. 2014d. *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 - Progress report*. ST 10097 2014 INIT, May 22. As of 12 October 2015: http://data.consilium.europa.eu/doc/document/ST-10097-2014-INIT/en/pdf

- Council of the European Union. 2015a. *EU Cybersecurity Strategy: Road map development*. As of 12 October 2015: http://www.statewatch.org/news/2015/apr/eu-council-cyber-security-roadmap-6183-rev1-15.pdf

- Council of the European Union. 2015b. 'Network and information security: breakthrough in talks with EP.' *Press Release* 538/15, 29 June. As of 12 October 2015: http://www.consilium.europa.eu/en/press/press-releases/2015/06/29-network-information-security/

- Council of the European Union. 2015c. *EU Internet Referral Unit at Europol – Concept note*. As of 12 October 2015: http://data.consilium.europa.eu/doc/document/ST-7266-2015-INIT/en/pdf

- Council of the European Union. 2015d. 'CEPOL: Council and Parliament agree on updated rules.' *Press Release* 544/15, 30 June. As of 12 October 2015: http://www.consilium.europa.eu/en/press/press-releases/2015/06/30-cepol-updated-rules/

- Court of Justice of the European Union. 2014. 'The Court of Justice declares the Data Retention Directive to be invalid.' *Press Release No 54/14*, April 8. As of 12 October 2015: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

- Czech National Security Centre (NCKB). 2015. *National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020*. National Security Authority (NBU). As of 12 October 2015: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_en.pdf, p. 9

- Donohue, Brian. 2013. 'The big four banking Trojans.' *Kaspersky Lab Daily*, October 21. As of 12 October 2015: https://blog.kaspersky.com/the-big-four-banking-trojans/

- Dourado, Eli & Andrea Castillo. 2015. 'Dozens of Federal Cybersecurity Offices Duplicate Efforts with Poor Coordination.' *Mercatus Center*, April 14. As of 12 October 2015: http://mercatus.org/publication/dozens-federal-cybersecurity-offices-duplicate-efforts-poor-coordination

- Doyle, Charles. 2014. *Cybercrime: An overview of the federal computer fraud and abuse statute and related federal criminal laws*. Congressional Research Service, October 15. As of 12 October 2015: https://www.fas.org/sgp/crs/misc/97-1025.pdf

- Drinkwater, Doug. 2014. 'EU's new cybercrime taskforce set to launch.' *SC Magazine UK*, July 21. As of 12 October 2015: http://www.scmagazineuk.com/eus-new-cybercrime-taskforce-set-to-launch/article/361822/

- Drinkwater, Doug. 2015. 'Finnish bank hit by DDoS attacks.' *SC Magazine UK,* January 8. As of 12 October 2015: http://www.scmagazineuk.com/finnish-bank-hit-by-ddos-attacks/article/391591/

- Dunn Cavelty, Myriam. 2013a. 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse.' *International Studies Review* 15: 105-122

- Dunn Cavelty, Myriam. 2013b. 'A Resilient Europe For An Open, Safe and Secure Cyberspace.' *UI Occasional Papers*, No. 23. As of 12 October 2015: http://www.ui.se/eng/upl/files/99632.pdf

- Dunn Cavelty, Myriam. 2014. 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities.' *Science and Engineering Ethics* 20(3): 701-715

- European Union Agency for Network and Information Security (ENISA). 2006. *CERT Cooperation and its Further Facilitation by Relevant Stakeholders*. As of 12 October 2015: https://www.enisa.europa.eu/activities/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders/at_download/fullReport

- ENISA. 2011. *A Flair for Sharing – Encouraging Information Exchange Between CERTs: A Study Into the Legal and Regulatory Aspects of Information Sharing and Cross-border Collaboration of National/Governmental CERTs in Europe*. As of 12 October 2015: https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing/legal-information-sharing-1/at_download/fullReport

- ENISA. 2013. *National-level Risk Assessments: An Analysis Report.* As of 12 October 2015: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report/at_download/fullReport

- ENISA. 2014. 'Fighting cybercrime: Strategic cooperation agreement signed between ENISA and Europol.' *Press Release*, June 26. As of 12 October 2015: http://www.enisa.europa.eu/media/press-releases/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol

- ENISA. 2015a. *ENISA Threat Landscape 2014*. As of 12 October 2015: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

- ENISA. 2015b. 'CERT.' As of 12 October 2015: http://www.enisa.europa.eu/activities/cert/sitemap

- ENISA. 2015c. 'CERT Inventory.' As of 12 October 2015: http://www.enisa.europa.eu/activities/cert/background/inv

- ENISA. 2015d. 'CERT Factsheet.' As of 12 October 2015: http://www.enisa.europa.eu/activities/cert/background/cert-factsheet

- ENISA. n.d. 'Cyber Atlantic 2011.' As of 12 October 2015: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011

- ENISA. n.d. 'First joint EU-US cyber security exercise conducted today.' *Press Release*, 3 November. As of 12 October 2015: https://www.enisa.europa.eu/media/press-releases/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011

- Eurojust. 2014a. 'Annual Report 2014.' As of 12 October 2015: http://www.eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202014/Annual-Report-2014-EN.pdf

- Eurojust. 2014b. 'International operation hits BlackShades users.' *Press Release*, May 19. As of 12 October 2015: http://www.eurojust.europa.eu/press/pressreleases/pages/2014/2014-05-19.aspx

- Eurojust. 2015a. 'Mission and tasks.' As of 12 October 2015: http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx

- Eurojust. 2015b. *Operation BlackShades: An Evaluation*. As of 12 October 2015: https://www.gccs2015.com/sites/default/files/documents/Bijlage%202%20-%20Eurojust%20(10%2004%2015)%20Blackshades-Case-Evaluation.pdf

- European Commission. 2010. 'Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats.' *Press Release*, April 14. As of 12 October 2015: http://europa.eu/rapid/press-release_MEMO-11-246_en.htm

- European Commission. 2011. *Report from the Commission to the Council and the European Parliament - Evaluation report on the Data Retention Directive (Directive 2006/24/EC).* COM (2011) 225 Final. As of 12 October 2015:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF

- European Commission. 2012a. 'Cyber security strengthened at EU institutions following successful pilot scheme.' *Press Release,* September 12. As of 12 October 2015: http://europa.eu/rapid/press-release_IP-12-949_en.htm

- European Commission. 2012b. 'EU and US launch Global Alliance to fight child sexual abuse online.' *Press Release*, June 21. As of 12 October 2015: http://europa.eu/rapid/press-release_IP-12-680_en.htm

- European Commission. 2013a. *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cyberstrategy of the European Union: An Open, Safe and Secure Cyberspace*. JOIN (2013) 1 Final. As of 12 October 2015: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

- European Commission. 2013b. *Proposal for a Directive of the European Parliament and the Council – Concerning measures to ensure a high common level of network and information security across the Union*. COM (2013) 48 Final. As of 12 October 2015: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

- 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*. COM (2013) 48 Final - 2013/0027 (COD). As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0048

- European Commission. 2014. 'Biggest ever cyber security exercise in Europe today.' *Press Release*, October 30. As of 12 October 2015: http://europa.eu/rapid/press-release_IP-14-1227_en.htm

- European Commission. 2015. *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions – The European Agenda on Security*. COM (2015) 185 Final. As of 12 October 2015: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

- European Commission. n.d.-a. 'Pillar III: Trust & Security.' *Digital Agenda for Europe*. As of 12 October 2015: http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security

- European Commission. n.d.-b. 'Digital Agenda in the Europe 2020 Strategy.' *Digital Agenda for Europe*. As of 12 October 2015: http://ec.europa.eu/digital-agenda/en/digital-agenda-europe-2020-strategy

- European Defence Agency (EDA). 2015a. *Cyber Defence Factsheet*. As of 12 October 2015: https://www.eda.europa.eu/docs/default-source/eda-factsheets/2015-02-10-factsheet_cyber-defence

- EDA. 2015b. 'Mission.' As of 12 October 2015: http://www.eda.europa.eu/Aboutus/Whatwedo/Missionandfunctions

- EDA. 2015c. 'European Parliament Exchange of Views on Cyber Defense.' As of 12 October 2015: http://www.eda.europa.eu/info-hub/news/2015/03/18/european-parliament-exchange-of-views-on-cyber-defence

- European Parliament. 2013a. *Resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. 2013/2606(RSP). As of 12 October 2015: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0376+0+DOC+XML+V0//EN

- European Parliament. 2013b. 'Procedure 2013/0027/COD - COM (2013) 48: 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.' As of 12 October 2015: http://eur-lex.europa.eu/procedure/EN/202368

- European Parliament. n.d. 'Procedure file: 2013/0091 European Union Agency for Law Enforcement Cooperation and Training (Europol).' As of 12 October 2015: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0091(COD)

- European Parliament. 2014a. *Legislative resolution of 13 March 2014 on the 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*. P7_TA(2014)0244, (COM (2013)0048 – C7-0035/2013 – 2013/0027(COD)). As of 12 October 2015: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0244&language=EN

- European Parliament. 2014b. *Legislative resolution of 25 February 2014 on the proposal for a regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA*. P7_TA(2014)0121 (COM(2013)0173 – C7-0094/2013 – 2013/0091(COD)). As of 12 October 2015: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0121&language=EN&ring=A7-2014-0096

- European Parliament. 2015a. 'Cyber-attacks: how to best protect the media and critical infrastructure.' As of 12 August 2015: http://www.europarl.europa.eu/news/en/news-room/content/20150526STO59635/html/Cyber-attacks-how-to-best-protect-the-media-and-critical-infrastructure

- European Parliament. 2015b. *Resolution on the European Agenda on Security*. 2015/2697(RSP), July 9. As of 12 October 2015:

http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2015-0269&format=XML&language=EN

- European Parliament and the Council of the European Union. 2002. Common regulatory framework for electronic communications networks and services (Framework Directive). Directive 2002/21/EC, 7 March. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0021

- European Parliament and Council of the European Union. 2004. *Establishing the European Network and Information Security Agency*. Regulation (EC) No 460/2004, 10 March. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004R0460

- European Parliament and Council of the European Union. 2008. *Amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration*. Regulation (EC) no. 1007/2008, 24 September. As of 12 October 2015: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF

- European Parliament and Council of the European Union. 2009. *Amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services*. Directive 2009/140/EC, 25 November. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0140

- European Parliament and Council of the European Union. 2011. *Amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration*. Regulation (EU) No 580/2011, 8 June. As of 12 October 2015: https://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1

- European Parliament and Council of the European Union. 2013a. O*n attacks against information systems and replacing Council Framework Decision 2005/222 JHA*. Directive 2013/40/EU, 12 August. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32013L0040

- European Parliament and Council of the European Union. 2013b. *Concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004*. Regulation (EU) no. 526/2013, May 21. As of 12 October 2015: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0526

- European Union Cybercrime Taskforce (EUCTF). 2014. *Directive on Network and Information Security*. Europol, Letter from Mr Lee Miles to Mr Datsikas (unclassified document). The Hague, April 24.

- European Union External Action (EEAS). 2014. 'Fact Sheet: EU-US cooperation on cyber security and cyberspace.' *EEAS*, March 26. As of 12 October 2015: http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf

- Europol. 2014a. *The Internet Organised Crime Threat Assessment (iOCTA)*. As of 12 October 2015: https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf

- Europol. 2014b. 'Expert international cybercrime taskforce is launched to tackle online crime.' *Press Release*, September 1. As of 12 October 2015: https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime

- Europol. 2014c. 'Worldwide Operation against Cybercriminals.' *Press Release*, May 19. As of 12 October 2015: https://www.europol.europa.eu/content/worldwide-operation-against-cybercriminals

- Europol. 2015a. 'Combating cybercrime in a digital age.' As of 12 October 2015: https://www.europol.europa.eu/ec3

- Europol. 2015b. 'Payment fraud.' As of 12 October 2015: https://www.europol.europa.eu/ec3/payment-fraud

- Europol. 2015c. 'High-tech crimes.' As of 12 October 2015. https://www.europol.europa.eu/ec3/high-tech-crimes

- Europol. 2015d. 'Child sexual exploitation.' As of 12 October 2015: https://www.europol.europa.eu/ec3/child-sexual-exploitation

- Europol. 2015e. 'Cyber intelligence.' As of 12 October 2015: https://www.europol.europa.eu/ec3/cyber-intelligence

- Europol. 2015f. 'Joint Cybercrime Action Taskforce (J-CAT).' As of 12 October 2015: https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat

- Europol. 2015g. 'Strategic analysis.' As of 12 October 2015: https://www.europol.europa.eu/ec3/strategic-analysis

- Europol. 2015h. 'Training and capacity building.' As of 12 October 2015: https://www.europol.europa.eu/ec3/training-and-capacity-building

- Europol. 2015i. 'Forensic expertise.' As of 12 October 2015: https://www.europol.europa.eu/ec3/forensic-expertise

- Europol. 2015j. 'Public awareness and prevention.' As of 12 October 2015: https://www.europol.europa.eu/ec3/public-awareness-and-prevention

- Europol. 2015k. 'Outreach and cooperation.' As of 12 October 2015: https://www.europol.europa.eu/ec3/outreach-and-cooperation

- Europol. 2015l. 'International Police Operation Targets Polymorphic Beebone Botnet.' *Press Release*, April 9. As of 12 October 2015: https://www.europol.europa.eu/content/international-police-operation-targets-polymorphic-beebone-botnet

- Europol. 2015m. 'Europol's Internet Referral Unit to combat terrorist and violent extremist propaganda.' *Press release*, 1 July. As of 12 October 2015: https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda

- Europol. n.d.-a. 'Agreements.' As of 12 October 2015: https://www.europol.europa.eu/category/news-category/agreements

- Europol. n.d.-b. 'Joint Investigation Teams (JITs).' As of 12 October 2015: https://www.europol.europa.eu/content/page/joint-investigation-teams-989

- Europol .n.d.-c. 'EC3 Programme Board.' As of 12 October 2015: https://www.europol.europa.eu/ec/ec3-board

- Farrell, Henry. 2015. 'What's New in the U.S. Cyber Strategy.' *The Washington Post,* April 24. As of 12 October 2015: http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/04/24/whats-new-in-the-u-s-cyber-strategy/

- Federal Bureau of Investigations (FBI). 2012. 'Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce 24 Arrests in Eight Countries as Part of International Cyber Crime Takedown.' *New York FBI Office*, June 26. As of 12 October 2015: https://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown

- FBI. 2014. 'International Blackshades Malware Takedown.' *Press Release*, May 19. As of 12 October 2015: https://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown

- FBI. 2015a. 'Private Industry Notification.' As of 12 October 2015: https://info.publicintelligence.net/FBI-BitcoinExtortionCampaigns.pdf

- FBI. 2015b. 'FBI Works with Foreign Partners to Target Botnet.' *Press Release*, April 9. As of 12 October 2015: https://www.fbi.gov/news/pressrel/press-releases/fbi-works-with-foreign-partners-to-target-botnet

- FBI. 2015c. 'Co-Creator of Blackshades Malware Pleads Guilty in Manhattan Federal Court.' *Press Release*, February 18. As of 12 October 2015: https://www.fbi.gov/newyork/press-releases/2015/co-creator-of-blackshades-malware-pleads-guilty-in-manhattan-federal-court

- FBI. 2015d. 'Swedish Co-Creator of Blackshades Malware That Enabled Users Around the World to Secretly and Remotely Control Victims' Computers Sentenced to 57 Months in Prison.' *Press Release*, June 23. As of 12 October 2015: https://www.fbi.gov/newyork/press-releases/2015/swedish-co-creator-of-blackshades-malware-that-enabled-users-around-the-world-to-secretly-and-remotely-control-victims-computers-sentenced-to-57-months-in-prison

- FBI. n.d. 'Addressing Threats to the Nation's Cybersecurity.' As of 12 October 2015: https://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1

- Felten, Ed. 2008. 'What's the Cyber in Cybersecurity?' *Freedom to Tinker,* July 24. As of 12 October 2015: https://freedom-to-tinker.com/blog/felten/whats-cyber-cyber-security/

- Ferguson, Rik. 2012. 'Don't be dumb, keep schtumm.' *TrendMicro Blog,* March 27. As of 12 October 2015: http://countermeasures.trendmicro.eu/dont-be-dumb-keep-schtumm/

- Field, Tom. 2013. 'Enisa Aims for Longer, Stronger Role: European Security Agency Extended, Strengthened by Parliament.' *Bank Info Security,* April 22. As of 12 October 2015: http://www.bankinfosecurity.com/interviews/enisa-aims-for-longer-stronger-role-i-1890

- Finklea, Kristin & Theohary, Catherine. 2015. *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. Congressional Research Service, January 15. As of 12 October 2015: https://www.fas.org/sgp/crs/misc/R42547.pdf

- FireEye. 2015. *Mixed state of readiness for New Cybersecurity regulations in Europe – French, German and UK organisations need more clarity on compliance requirements for 2015-2017*. As of 12 October 2015: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/rpt-mixed-state-of-readiness-for-new-cybersecurity-regulations-in-europe.pdf

- Fischer Eric A. & Stephanie M Logan. 2015. *Cybersecurity and information sharing: Comparison of House and Senate bills in the 114th Congress*. Congressional Research Service, August 5. As of 12 October 2015: https://www.fas.org/sgp/crs/misc/R44069.pdf

- Fleming, Jeremy. 2015. 'Cyber security directive held up in face of wild west internet.' *Euractiv,* April 1. As of 12 October 2015: http://www.euractiv.com/sections/infosociety/cyber-security-directive-held-face-wild-west-internet-313431

- Fleming Matthew H. & Eric Goldstein. 2012. *An analysis of the primary authorities governing and supporting the efforts of the department of homeland security to secure the cyberspace of the United States.* As of 12 October 2015: http://ssrn.com/abstract=2182675

- FP Staff. 2015. 'The dawn of ransomwear: How ransomware could move to wearable devices.' *First Post*, August 10. As of 12 October 2015: http://www.firstpost.com/business/dawn-ransomwear-ransomware-move-wearable-devices-2385712.html

- Gara, Tom. 2014. 'October 2015: The End of the Swipe-and-Sign Credit Card.' *The Wall Street Journal*, 6 February. As of 12 October 2015: http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/

- Gehem et al. 2015. *Assessing cyber security – A meta-analysis of threats, trends, and responses to cyber attacks*. The Hague: The Hague Center for Strategic Studies. As of 12 October 2015: http://www.hcss.nl/reports/download/164/2938/

- Gerden, Eugene. 2015. 'FINcert to help Russian banks respond to cyber attacks.' *SC Magazine UK,* July 10. As of 12 October 2015: http://www.scmagazineuk.com/fincert-to-help-russian-banks-respond-to-cyber-attacks/article/425701/

- Geuss, Megan. 2015. 'Paying $20 to delete your Ashley Madison profile was probably a bad idea.' *Arstechnica*, July 10. As of 12 October 2015: http://arstechnica.com/business/2015/07/cheaters-hook-up-site-ashley-madison-makes-account-deletion-confusing/

- Global Conference on Cyberspace (GCCS). 2015. *Chair's Statement*. As of 12 October 2015: https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf

- Global Network Initiative. 2015. *Data Beyond Borders – Mutual Legal Assistance in the Internet Age*. As of 12 October 2015: http://csis.org/files/attachments/GNI%20MLAT%20Report.pdf

- Hattem, Julian. 2014. 'Report calls 2013 year of the mega breach.' *The Hill*, August 4. As of 12 October 2015: http://thehill.com/policy/technology/202913-report-calls-2013-year-of-the-mega-breach

- Heickero, Roland. 2014. 'Cyber Terrorism: Electronic Jihad.' *Strategic Analysis* 38(4): 554-565

- Heise Online. 2014. 'Ermittlungen wegen "Blackshades" -Trojaner in Deutschland.' *Heise Online*, May 22. As of 12 October 2015: http://www.heise.de/newsticker/meldung/Ermittlungen-wegen-Blackshades-Trojaner-in-Deutschland-2195984.html

- Herr, Trey & Allan Friedman. 2015. 'Redefining Cybersecurity.' *The American Foreign Policy Council Defense Technology Program Brief*, January 22. As of 12 October 2015: http://www.afpc.org/publication_listings/viewPolicyPaper/2664

- Hesseldahl, Arik. 2015. 'Why the Federal Government sucks at Cyber Security.' *re/code*, 23 June. As of 12 October 2015: http://recode.net/2015/06/23/why-the-federal-government-sucks-at-cybersecurity/

- Hirst, Nicholas. 2015. 'US Tech Firms targeted in Cybersecurity Talks.' *Politico*, May 21. As of 12 October 2015: http://www.politico.eu/article/another-path-to-cybersecurity/

- Hoffman, Bruce, Edwin Meese & Timothy Roemer. 2015. *The FBI: Protecting the Homeland in the 21st Century*. Report of the Congressionally-directed 9/11 Review Commission. As of 12 October 2015: https://www.fbi.gov/stats-services/publications/protecting-the-homeland-in-the-21st-century

- Howorth, Jolyon. 2012. 'European defense policy needs recalibration.' *Foreign Policy*, June 29. As of 12 October 2015: http://foreignpolicy.com/2012/06/29/european-defense-policy-needs-recalibration/

- InfoSec Institute. 2014. 'Domain Generation Algorithm (DGA).' *General Security*, 23 June. As of 12 October 2015: http://resources.infosecinstitute.com/domain-generation-algorithm-dga/

- Intel Security. 2014. *Catch Me if You Can - Antics of a Polymorphic Botnet*. As of 12 October 2015: http://www.mcafee.com/us/resources/misc/infographic-catch-me-if-you-can.pdf

- Internet Crime Complaint Center (IC3). n.d. 'About Us.' As of 12 October 2015: http://www.ic3.gov/about/default.aspx

- Jackson, Brian. 2014. *How Do We Know What Information Sharing Is Really Worth?* Santa Monica, Calif.: RAND Corporation. As of 12 October 2015: http://www.rand.org/pubs/research_reports/RR380.html

- Jardine, Eric. 2015. Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime. *Global Commission on Internet Governance*, No. 16. As of 12 October 2015: https://www.cigionline.org/sites/default/files/no16_web_0.pdf

- Johnston, Jules. 2015. 'Bettel Calls for EU Cyber Plan by Year's End.' *Politico*, June 10. As of 12 August 2015: http://www.politico.eu/article/xavier-bettel-cybersecurity-matters/

- Kent, Gail. 2014. Sharing Investigation-specific data with law enforcement – an international approach. *Stanford Public Law Working Paper.* As of 12 October 2015: http://ssrn.com/abstract=2472413

- Keyser, Mike. 2003. The Council of Europe Convention on Cybercrime. *Journal of Transnational Law and Policy* 12(2): 287-326

- Kharpal, Arjun. 2015. 'Year of the hack? A billion records compromised in 2014.' *CNBC,* February 12. As of 12 October 2015:

http://www.cnbc.com/2015/02/12/year-of-the-hack-a-billion-records-compromised-in-2014.html

- Kissel, Richard. 2013. *Glossary of Key Information Security Terms*. National Institute of Standards and Technology (NIST), NISTIR 7298 Revision 2. As of 12 October 2015: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

- Kirk, Jeremy. 2015. 'Swedish man pleads guilty to peddling Blackshades malware.' *CIO*, February 18. As of 12 October 2015: http://www.cio.com/article/2886453/swedish-man-pleads-guilty-to-peddling-blackshades-malware.html

- Klimburg, Alexander & Heli Tirmaa-Klaar. 2011. *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*. Study for the European Parliament's Subcommittee on Security and Defence. As of 12 October 2015: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf

- Klimburg, Alexander. 2015. 'Here's Where Europe Has Made Big Changes in Cyber Security.' *DefenseOne,* February 3. As of 12 October 2015: http://www.defenseone.com/threats/2015/02/heres-where-europe-has-made-big-changes-cyber-security/104454/

- Krebs, Brian. 2012. 'Microsoft Responds to Critics over Botnet Bruhaha.' *KrebsonSecurity*, 16 April. As of 12 October 2015: http://krebsonsecurity.com/2012/04/microsoft-responds-to-critics-over-botnet-bruhaha/

- Krebs, Brian. 2015a. 'Online cheating site Ashley Madison hacked.' *KrebsonSecurity,* July 15. As of 12 October 2015: http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/

- Kujawa, Adam. 2012. 'You Dirty RAT! Part 2 – BlackShades NET.' *Malwarebytes*, June 15. As of 12 October 2015: https://blog.malwarebytes.org/intelligence/2012/06/you-dirty-rat-part-2-blackshades-net/

- Lagrimas, Dianne. 2015. 'Beebone Botnet Takedown: Trend Micro Solutions.' *Trend Micro - Threat Encyclopedia*. As of 12 October 2015: http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions

- Lavasoft. n.d. 'Malware from A to Z.' As of 9 September 2015: http://lavasoft.com/mylavasoft/securitycenter/spyware-glossary#RAT

- Law Enforcement and Prosecutors Conference on Cyber Crime. 2015. Joint Conference Paper. *LEAP2015*, 15 April. As of 12 October 2015: https://www.gccs2015.com/sites/default/files/documents/JOINT%20CONFERENCE%20PAPER%20LEAP2015final.doc

- Lawson, Sean. 2011. 'DOD's "First" Cyber Strategy is Neither First, Nor a Strategy.' *Forbes,* August 1. As of 12 October 2015: http://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/

- Lemos, Robert. 2015. 'Joint international Effort Disrupts Beebone Botnet.' *eWeek.com*, April 9. As of 12 October 2015: http://www.eweek.com/security/joint-international-effort-disrupts-beebone-botnet.html

- Levin, Avner & Paul Goodrick. 2013. 'From cybercrime to cyberwar? The international policy shift and its implications for Canada.' *Canadian Foreign Policy Journal* 19(2): 127-143

- Lewis, Dave. 2015. 'DDoS attacks have graduated to extortion.' *Huffington Post,* June 23. As of 12 October 2015: http://www.huffingtonpost.com/dave-lewis2/ddos-attacks-have-graduat_b_7639516.html

- Libicki, Martin C. 2015. *Sharing Information about Threats is not a Cybersecurity Panacea*. Santa Monica, Calif.: RAND Corporation. CT-425. As of 12 October 2015: http://docs.house.gov/meetings/HM/HM08/20150304/103055/HHRG-114-HM08-Wstate-LibickiM-20150304.pdf

- Libicki, Martin C., Lilian Ablon & Tim Webb. 2015. *Defender's Dilemma: Charting a Course Toward Cyber Security*. Santa Monica, Calif.: RAND Publications. As of 12 October 2015: http://www.rand.org/pubs/research_reports/RR1024.html

- Limnell, Jarno. 2015. 'Europe Must Play Stronger Role in Cyber Security.' *Euobserver*, July 10. As of 12 October 2015: https://euobserver.com/opinion/129560

- Lowery, Edward W. 2014. *Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to support the DHS Cyber Security Mission*. Monterey, Calif.: Naval Postgraduate School. As of 12 October 2015; https://www.hsdl.org/?view&did=762425

- Lyne, James. 2015. *Security Threat Trends 2015.* Sophos. As of 12 October 2015: https://www.sophos.com/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf

- Malmström, Cecilia. 2013. *Next step in the EU-US cooperation on Cyber security and Cybercrime*. Speech at the Homeland Security Policy Institute, George Washington University, 30 April. As of 12 October 2015: http://europa.eu/rapid/press-release_SPEECH-13-380_en.doc

- Maude, James. 2015. 'File less fears.' *Avecto Blog*, 1 May. As of 12 October 2015: https://blog.avecto.com/2015/05/file-less-fears/

- McAfee. n.d. 'Glossary of Technical Terms.' As of 12 October 2015: https://kc.mcafee.com/corporate/index?page=glossary

- McAfee. 2011. *Combating Advanced Persistent Threats – How to prevent, detect, and remediate APTs*. As of 12 October 2015: http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf

- McNeal, Gregory S. 2014. 'Controversial Cybersecurity Bill Known As CISA Advances Out Of Senate Committee.' *Forbes*, July 9. As of 12 October 2015: http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/

- Meisner, Jeffrey. 2012. 'Microsoft and Financial Services Industry Leaders target Cybercriminal Operations form Zeus Botnets.' *Microsoft News Center*, 25 March. As of 12 October 2015: http://blogs.microsoft.com/blog/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets/

- MicroData. 2015. 'Malvertisement Alert! Firefox and IE Users affected.' *MicroData Blog*, 4 February. As of 12 October 2015: http://blog.microdata.com/malvertisement-alert-firefox-and-ie-users-affected/

- Microsoft. n.d. 'The Exploit Malware Family.' Microsoft Malware Protection Center. As of 12 October 2015: http://www.microsoft.com/security/portal/mmpc/threat/exploits.aspx

- Microsoft. n.d. 'Malware Protection Center – Glossary.' As of 12 October 2015: https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx

- National Cyber Security Centre (NCSC). 2014. *Cyber Security Assessment Netherlands – CSBN 4*. As of 12 October 2015: https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/cyber-securty-assessment-netherlands-4-cybercrime-and-digital-espionage-remain-the-biggest-threat/1/CSAN%2B4.pdf

- National Initiative for Cybersecurity Careers and Studies (NICCS). n.d. 'Explore Terms: A Glossary of Common Cybersecurity Terminology.' As of 12 October 2015: https://niccs.us-cert.gov/glossary#capability

- National Institute of Standards and Technology (NIST). 2001. *Announcing the Advanced Encryption Standard*. FIPS PUB 197, November 26. As of 12 October 2015: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

- National Institute of Standards and Technology (NIST). 2004. *Standards for Security Categorization of Federal Information and Information Systems*. FIPS PUB 199. As of 12 October 2015: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

- National Institute of Standards and Technology (NIST). 2006. *Minimum security requirements for federal information and information systems*. FIPS

PUB, 9 March. As of 12 October 2015: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

- National Institute of Standards and Technology (NIST). 2010. *Guide for Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*. NIST Special Publication 800-53A. As of 12 October 2015: http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

- Neutze, Jan. 2014. 'Cybersecurity in Europe – an opportunity (about to be) missed.' *Microsoft EU Policy Blog*, October 24. As of 12 October 2015: http://blogs.microsoft.com/eupolicy/2014/10/24/cybersecurity-in-europe-an-opportunity-about-to-be-missed/

- Norton. n.d. 'Glossary.' As of 12 October 2015: http://us.norton.com/security_response/glossary/define.jsp?letter=p&word=patch

- North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2013. 'ENISA's new mandate to face cyber security challenges.' As of 12 October 2015: https://ccdcoe.org/enisas-new-mandate-face-cyber-security-challenges.html

- NATO CCDCOE. 2014. 'Developments in the European Union: NIS Directive, data protection reform, EP's response to U.S. surveillance.' As of 12 October 2015: https://ccdcoe.org/developments-european-union-nis-directive-data-protection-reform-eps-response-us-surveillance.html

- NATO CCDCOE. 2015. 'Cyber definitions.' As of 12 October 2015: https://ccdcoe.org/cyber-definitions.html

- Nye, Joseph S. 2014. The Regime complex for managing global cyber activities. *Global Commission on Internet Governance*, No. 1. As of 12 August 2015: https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

- Openbaar Ministerie. 2014. 'Wereldwijde actie politie en justitie tegen hackers.' As of 12 October 2015: https://www.om.nl/vaste-onderdelen/zoeken/@85963/wereldwijde-actie/

- Open Rights Group. 2015. *Data retention in the EU following the CJEU ruling – updated April 2015*. As of 12 October 2015: https://www.openrightsgroup.org/assets/files/legal/Data_Retention_status_table_updated_April_2015_uploaded_finalwithadditions.pdf

- O'Murchu, Liam & Fred P. Gutierrez. 2015. *The evolution of the fileless click-fraud malware Poweliks*. Symantec Security Response. As of 12 October 2015: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/evolution-of-poweliks.pdf

- Organisation for Economic Co-operation and Development (OECD). 2012. *Cybersecurity Policy Making at a Turning Point*. As of 12 October 2015: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

- Osborne, Charlie. 2015. 'Retailers targeted by new point-of-sale malware through job requests.' *ZDnet*, May 26. As of 12 October 2015: http://www.zdnet.com/article/internships-become-bait-to-infect-retailers-with-new-point-of-sale-malware/

- Pearse, Ryan, Buckenham, Paddy & Donnelly, Niall. 2014. *EU Network and Information Security Directive: Is It Possible to Legislate For Cyber Security?* Arthur Cox, Group Briefing. As of 12 October 2015: http://www.arthurcox.com/wp-content/uploads/2014/10/Arthur-Cox-EU-Network-and-Information-Security-Directive-October-2014.pdf

- Pescatore, John. 2014. *2014 Trends That Will Reshape Organizational Security*. As of 12 October 2015: https://www.sans.org/reading-room/whitepapers/analyst/2014-trends-reshape-organizational-security-34625

- Pinson, Richard. 2015. 'Computer threat: Cryptolocker virus is ransomware.' *Nashville Business Journal*, August 10. As of 12 October 2015: http://www.bizjournals.com/nashville/blog/2015/08/computer-threat-cryptolocker-virus-is-ransomware.html

- Ponemon Institute. 2014. 'Ponemon Institute releases 2014 Cost of Data Breach: Global Analysis.' *Ponemon Institute Blog*, August 26. As of 12 October 2015: http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

- Ponemon Institute. 2015. *2014: A year of mega breaches*. As of 12 October 2015: http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf

- Praxiom Research Group Limited. 2013. 'Plain English ISO IEC 27000 2014 Information Security Definitions. 2014.' As of 12 October 2015: http://www.praxiom.com/iso-27000-definitions.htm

- Quinn, Richard. 2014. 'Statement before the House Homeland Security Committee, Subcommittee on Cyber Security, Infrastructure Protection, and Security Technologies.' *FBI Testimony*, April 16. As of 12 October 2015: https://www.fbi.gov/news/testimony/the-fbis-role-in-cyber-security

- Ragan, Steve. 2013. 'NBC cleans up site after citadel compromise.' *Securityweek.com*, 22 February. As of 12 October 2015: http://www.securityweek.com/nbc-cleans-site-after-citadel-compromise

- Rains, Tim. 2013. 'Ransomware is on the Rise, Especially in Europe.' *Microsoft Blog,* November 19. As of 12 October 2015:

http://blogs.microsoft.com/cybertrust/2013/11/19/ransomware-is-on-the-rise-especially-in-europe/

- Rajan, Nitya. 2015. 'Ashley Madison hack threatens to expose millions.' *The Huffington Post*, July 20. As of 12 October 2015: http://www.huffingtonpost.co.uk/2015/07/20/ashley-madison-hack-affairs-website-_n_7830480.html

- Reeve, Tom. 2015. 'EC report: Cyber-crime demands a new approach to law enforcement.' *SC Magazine UK*, April 29. As of 12 October 2015: http://www.scmagazineuk.com/ec-report-cyber-crime-demands-a-new-approach-to-law-enforcement/article/411748/

- Rijksoverheid. 2014. *Antwoorden Kamervragen over het hacken van servers door de politie*. As of 12 October 2015: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/10/18/antwoorden-kamervragen-over-het-hacken-van-servers-door-de-politie-terwijl-de-zogenaamde-hackwet-nog-niet-door-de-kamer-is-beha

- Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle & Pablo Rodriquez. 2013. *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)*. Santa Monica, Calif.: Rand Corporation. As of 12 October 2015: http://www.rand.org/pubs/research_reports/RR286.html

- Robinson, Neil, Horvath, Veronika, Cave, Jonathan, Roosendaal, Arnold & Klaver, Marieke. 2013. *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts*. European Parliament, Directorate-General for Internal Policies – Policy Department A: Economic and Scientific Policy. As of 12 October 2015: http://www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE_NT(2013)507476_EN.pdf

- Rouse, Margaret & Matthew Haugh. 2015. 'POS malware (point-of-sale malware).' *WhatIS.com*, January. As of 12 October 2015: http://whatis.techtarget.com/definition/POS-malware-point-of-sale-malware

- Rouse, Margaret. n.d. 'Memory-scraping Malware.' As of 12 October 2015: http://searchsecurity.techtarget.com/definition/memory-scraping-malware

- Samani, Raj & Weafer, Vincent. 2015. 'Takedown Stops Polymorphic Botnet.' *McAfee Labs*. April 9. As of 12 October 2015: https://blogs.mcafee.com/mcafee-labs/takedown-stops-polymorphic-botnet

- Samani, Raj. 2015. 'Update on Beebone Botnet Takedown.' *McAfee Labs*, April 20. As of 12 October 2015: https://blogs.mcafee.com/mcafee-labs/beebone-update

- Sandee, Michael. 2012. 'Critical analysis of Microsoft Operation B71.' *Fox-IT International Blog*, 12 April. As of 12 October 2015: http://blog.fox-it.com/2012/04/12/critical-analysis-of-microsoft-operation-b71/

- Sanger, David. 2015. 'Pentagon Announces New Strategy for Cyberwarfare.' *The New York Times*, April 24. As of 12 October 2015: http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html

- Segura, Jerome. 2015. 'Large Malvertising Campaign goes (almost) undetected.' *Malwarebytes.com*, 14 September. As of 12 October 2015: https://blog.malwarebytes.org/malvertising-2/2015/09/large-malvertising-campaign-goes-almost-undetected/

- Shadowserver Foundation. 2015a. 'AAEH/Beebone Botnet.' As of 12 October 2015: https://aaeh.shadowserver.org/

- Shooter, Simon, Joseph Jackson & Toby Bond. n.d. 'Cybersecurity and the EU: regulating for network security.' *Bird & Bird*. As of 12 October 2015: http://www.twobirds.com/~/media/PDFs/News/CybersecurityandtheEU06201300125701.pdf

- Shooter, Simon. 2014a. 'MEPs vote strongly in favour of the proposed European Cybersecurity Directive.' *Bird&Bird*, March 13. As of 12 October 2015: http://www.lexology.com/library/detail.aspx?g=c39213ca-77b0-432e-943e-37854fc6b921

- Shooter, Simon. 2014b. 'European Cybersecurity Directive Moves Closer to Becoming a Reality.' *Bird & Bird*, February 17. As of 12 October 2015: http://www.twobirds.com/en/news/articles/2014/global/european-cybersecurity-directive-moves-closer-to-becoming-a-reality?utm_source=Concep%20Send&utm_medium=email&utm_campaign=MEPs%20vote%20strongly%20in%20favour%20of%20the%20proposed%20European%20Cybersecurity%20Directive_03/13/2014

- Silva, Karine E. 2013. 'Europe's fragmented approach towards cyber security.' *Internet Policy Review* 2(4). As of 12 October 2015: http://policyreview.info/articles/analysis/europes-fragmented-approach-towards-cyber-security

- Simmons, Dan. 2015. 'Europol kills off shape-shifting "Mystique" malware.' *BBC,* April 9. As of 12 October 2015: http://www.bbc.co.uk/news/technology-32218381

- Sternstein, Aliya. 2015. 'Senators want Homeland Security to be a leading cyber defense agency.' *DefenseOne*, 22 July. As of 12 October 2015: http://www.defenseone.com/technology/2015/07/senators-want-homeland-security-be-leading-cyber-defense-agency/118410

- Sukhovey, Darya & Miroshnichenko, Olga. 2014. 'American Political Experts on Cyber Security.' *World Applied Sciences Journal* 31(4): 559-561

- Symantec. 2013. 'Blackshades Rat Usage on the Rise Despite Author's Alleged Arrest.' *Security Response Blog*, November 25. As of 12 October 2015: http://www.symantec.com/connect/blogs/blackshades-rat-usage-rise-despite-

author-s-alleged-arrest

- Tamir, Dana. 2014. 'ZeuS.Maple variant targets Canadian online banking customers.' *Security Intelligence*, June 9. As of 12 October 2015: https://securityintelligence.com/zeus-maple-variant-targets-canadian-online-banking-customers/#.VczBw01RHcs

- Tehan, Rita. 2015. *Cybersecurity: Authoritative Reports and Resources, by Topic.* Congressional Research Service, April 28. As of 12 October 2015: https://www.fas.org/sgp/crs/misc/R42507.pdf

- Thierer, Adam. 2013. 'Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle.' *Minnesota Journal of Law, Science and Technology 14(1)*: 309-386.

- TrendMicro. n.d. 'Definition: Ransomware.' As of 12 October 2015: http://www.trendmicro.com.au/vinfo/au/security/definition/ransomware

- TrendMicro. n.d. 'Malvertisement definition.' As of 2 October, 2015: http://www.trendmicro.com/vinfo/us/security/definition/Malvertisement

- TrendMicro. n.d. 'Threat Encyclopedia – Watering Hole 101.' As of 12 October 2015: http://www.trendmicro.com.au/vinfo/au/threat-encyclopedia/web-attack/137/watering-hole-101

- Trustwave. 2014. *White Paper: Combatting Point of Sale Malware*. As of 12 October 2015: http://www2.trustwave.com/rs/trustwave/images/Special_Report_Combatting_Point_of_Sale_Malware.pdf

- United States Air Force. n.d. 'USCYBERCOMMAND Cyber Mission Force.' Headquarters US AirForce, Power Point Presentation. As of 12 October 2015: http://www.safcioa6.af.mil/shared/media/document/AFD-140512-039.pdf

- United States Congress. 2014. *S.2588 - Cybersecurity Information Sharing Act of 2014*. As of 12 October 2015: https://www.congress.gov/bill/113th-congress/senate-bill/2588

- United States Department of Defense (US DoD). 2011. *Department of Defense Strategy for Operating in Cyberspace*. As of 12 October 2015: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

- US DoD. 2015a. *The DoD Cyber Strategy*. As of 12 October 2015: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

- US DoD. 2015b. 'Fact Sheet: Department of Defense Cyber Strategy.' As of 12 October 2015: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf

- United States Department of Homeland Security (US DHS). 2009. *Strategy for Securing Control Systems – Coordinating and Guiding Federal, State and Private Sector Initiatives*. As of 12 October 2015: https://ics-cert.us-cert.gov/sites/default/files/documents/Strategy%20for%20Securing%20Control%20Systems.pdf

- US DHS. 2010. 'Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity.' As of 12 October 2015: http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf

- US DHS. 2013a. *Written testimony of DHS Deputy Secretary Jane Holl Lute for a House Committee on Homeland Security hearing titled 'DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure*.' As of 12 October 2015: http://www.dhs.gov/news/2013/03/13/written-testimony-dhs-deputy-secretary-jane-holl-lute-house-committee-homeland

- US DHS. 2013b. 'DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers.' As of 12 October 2015: https://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-02_Oct13.pdf

- US DHS. 2013c. 'DHS/NPPD/PIA-001 The Einstein Program.' As of 12 October 2015: http://www.dhs.gov/publication/dhsnppdpia-001the-einstein-program

- US DHS. 2014. *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 titled 'Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future*.' As of 12 October 2015: http://www.dhs.gov/news/2014/05/07/written-testimony-usss-cyber-operations-branch-senate-appropriations-subcommittee

- US DHS. 2015a. *Written testimony of DHS Secretary Jeh Johnson for a House Committee on the Judiciary hearing titled 'Oversight of the U.S. Department of Homeland Security*.' As of 12 October 2015: http://www.dhs.gov/news/2015/07/14/written-testimony-dhs-secretary-johnson-house-committee-judiciary-hearing-titled-

- US DHS. 2015b. 'About the Critical Infrastructure Cyber Community C3 Voluntary Program.' As of 12 October 2015: http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program

- US DHS. 2015c. 'Einstein 3 Accelerated.' As of 12 October 2015: http://www.dhs.gov/publication/einstein-3-accelerated

- US DHS. 2015d. 'DHS Unveils Major Expansion of Ice Cyber Crimes Center.' *Press Release*, July 22. As of 12 October 2015: http://www.dhs.gov/news/2015/07/22/dhs-unveils-major-expansion-ice-cyber-crimes-center

- US DHS. 2015e. *Remarks by Secretary of Homeland Security Jeh Johnson at the RSA Conference 2015*. As of 12 October 2015: http://www.dhs.gov/news/2015/04/21/remarks-secretary-homeland-security-jeh-johnson-rsa-conference-2015

- United States Department of Justice (US DoJ). 2014a. '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.' *Press Release*, May 19. As of 12 October 2015: http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection

- US DoJ. 2014b. *United States of America v. Kyle Fedorek*. As of 12 October 2015: http://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Blackshades,%20Fedorek%20Complaint%2014%20Mag.%201064_0.pdf

- US DoJ. 2015a. 'Major computer hacking forum dismantled.' *Justice News*, July 15. As of 12 October 2015: http://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled

- US DoJ. 2015b. *FY 2015 Budget Request – Mutual Legal Assistance Treaty Process Reform*. As of 12 October 2015: http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf

- US DoJ. n.d. 'Computer Crime and Intellectual Property Section (CCIPS).' As of 12 October 2015: http://www.justice.gov/criminal-ccips

- United States District Court, Eastern District of New York. 2012. *Microsoft Corp., FS-ISAC INC., and National Automated Clearing House Association v. John Does 1-39*. As of 12 October 2015: http://www.zeuslegalnotice.com/images/Ex_Parte_Application.pdf

- United States Government and Accountability Office (US GAO). 2011. *Defense Department Cyber Efforts: DOD Faces Challenges in its Cyber Activities*. As of 12 October 2015: http://www.gao.gov/assets/330/321818.pdf

- US GAO. 2013. *A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges*. As of 12 October 2015: http://www.gao.gov/assets/660/652817.pdf

- US GAO. 2015. *High Risk Series: An Update*. As of 12 October 2015: http://www.gao.gov/assets/670/668415.pdf

- United States House of Representatives. 2013. *Joint hearing before the Subcommittee on Emergency Preparedness, Response, and Communications and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security House of Representatives*. As of 12 October 2015:

http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg87116/pdf/CHRG-113hhrg87116.pdf

- United States Joint Chiefs of Staff. 2013. *Cyberspace Operations*. Joint Publication 3-12(R), 5 February. As of 12 October 2015: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

- United States Office of Personnel Management. 2015. 'OPM to Notify Employees of Cybersecurity Incident.' *Press Release*, June 4. As of 12 October 2015: https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/

- US Strategic Command. 2015. 'US Cyber Command.' As of 12 October 2015: https://www.stratcom.mil/factsheets/2/Cyber_Command/

- US-CERT. 2015. 'Alert (TA15-098A) AAEH.' As of 12 October 2015: https://www.us-cert.gov/ncas/alerts/TA15-098A

- Van der Meulen, Nicole S. 2011. 'Between Awareness and Ability: Consumers and financial identity theft.' *Communications & Strategies* 81.

- Van der Meulen, Nicole S. 2013. 'Following in the footsteps of terrorism? Cybersecurity as a crowded policy implementation space.' *Canadian Foreign Policy Journal* 19(2).

- Verizon. 2014. *2014 Data Breach Investigations Report.* As of 12 October 2015: http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf

- Verizon. 2015. *2015 Data Breach Investigations Report.* As of 12 October 2015: http://www.verizonenterprise.com/DBIR/2015/

- Wei, Wang. 2014. 'FBI raids BlackShades RAT Malware Customers in Europe and Australia.' *HackerNews*, May 16. As of 12 October 2015: http://thehackernews.com/2014/05/fbi-raids-blackshades-rat-malware_16.html

- Weidenholzer, Josef. 2014. 'European Union Agency for Law Enforcement Co-operation and Training (Europol).' *S&D Newsroom*, 24 February. As of 12 October 2015: http://www.socialistsanddemocrats.eu/content/european-union-agency-law-enforcement-co-operation-and-training-europol

- White House. 1998. *Presidential Decision Directive/NSC-63*. As of 12 October 2015: http://fas.org/irp/offdocs/pdd/pdd-63.htm

- White House. 2003. *The National Strategy to Secure Cyberspace.* As of 12 October 2015: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

- White House. 2009. *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communication Infrastructure*. As of 12 October 2015:

https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

- White House. 2010. 'Memorandum for the Heads of Executive Departments and Agencies.' *Office of Management and Budget*, July 6. As of 12 October 2015: https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf

- White House. 2013a. 'Executive Order – Improving Critical Infrastructure Cybersecurity.' *Office of the Press Secretary*, February 12 As of 12 October 2015: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

- White House. 2013b. *Liberty and Security in a Changing World – Report and Recommendations of the President's Review Group on Intelligence and Communication Technologies*. As of 12 October 2015: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

- White House. 2015a. 'Fact sheet: Enhancing and Strengthening the Federal Government's Cybersecurity.' *Office of Management and Budget*, June 12. As of 12 October 2015: https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf

- White House. 2015b. 'Fact Sheet: Executive order promoting private sector cybersecurity information sharing.' *Office of the Press Secretary*, February 12. As of 12 October 2015: https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform

- White House. 2015c. 'Statement of Administration Policy: H.R. 2596 – Intelligence Authorization Act for FY 2016.' *Office of Management and Budget*, June 15. As of 12 October 2015: https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saphr2596r_20150615.pdf

- White House. n.d.-a. 'The Comprehensive National Cybersecurity Initiative.' As of 12 October 2015: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

- White House. n.d.-b. 'FACT Sheet, U.S.-EU Cyber cooperation.' *Office of the Press Secretary*, March 26. As of 12 October 2015: https://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation

- Young, Joseph. 2015a. 'Hong Kong banks targeted by DDoS attack.' *BitCoinMagazine*, May 18. As of 12 October 2015: https://bitcoinmagazine.com/20449/hong-kong-banks-targeted-ddos-attacks-bitcoin-payout-demanded/

- Young, Mark. 2015b. 'Update on the cybersecurity directive – over to Luxembourg?' *The National Law Review,* June 15. As of 12 October 2015: http://www.natlawreview.com/article/update-cybersecurity-directive-over-to-luxembourg

- Zetter, Kim. 2015. 'Dozens nabbed in takedown of cybercrime forum Darkode.' *Wired*, July 15. As of 12 October 2015: http://www.wired.com/2015/07/dozens-nabbed-takedown-cybercrime-forum-darkode/

- Zheng, Denise & James Lewis. 2015. *Cyber Threat Information Sharing - Recommendations for Congress and the Administration.* Centre for Strategic and International Studies (CSIS). As of 12 October 2015: http://csis.org/files/publication/150310_cyberthreatinfosharing.pdf

- Zorabedian, John. 2014. 'How malware works: Anatomy of a drive-by download web attack (infographic).' *Sophos*, 26 March. As of 12 October 2015: https://blogs.sophos.com/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/