European Parliament

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

The law enforcement challenges of cybercrime: are we really playing catch-up?

Study for the LIBE Committee

EN

2015

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

The law enforcement challenges of cybercrime: are we really playing catch-up?

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. With a number of high-profile criminal cases, such as 'Silk Road', cybercrime has been very much in the spotlight in recent years, both in Europe and elsewhere. While this study shows that cybercrime poses significant challenges for law enforcement, it also argues that the key cybercrime concern for law enforcement is legal rather than technical and technological. The study further underlines that the European Parliament is largely excluded from policy development in the field of cybercrime, impeding public scrutiny and accountability.

DOCUMENT REQUESTED BY THE
COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

AUTHOR(S)

Dr. Ben Hayes, Researcher with Statewatch and Fellow at the Transnational Institute (TNI)

Dr. Julien Jeandesboz, Assistant Professor in Political Science at the University of Amsterdam (UvA) and Associate Researcher at the Centre d'Études sur les Conflits, Liberté et Sécurité (CCLS)

Dr. Francesco Ragazzi, Assistant Professor in International Relations at Leiden University (Netherlands) and Associate Researcher at the Centre d'Études sur les Conflits, Liberté et Sécurité (CCLS)

Dr. Stephanie Simon, Researcher in Political Science at the University of Amsterdam (UvA)

Prof. Valsamis Mitsilegas, Professor of European Criminal Law and Director of the Criminal Justice Centre at Queen Mary University of London

This Study was coordinated by the Centre d'Études sur les Conflits, Liberté et Sécurité (**CCLS**) and the Centre for European Policy Studies (**CEPS**) and conducted under the scientific supervision of **Prof. Didier Bigo** (Director of CCLS and Professor at Sciences Po Paris and King's College London) and **Dr. Amandine Scherrer** (European Studies Coordinator and Associate Researcher at CCLS).
The authors would like to express their gratitude to **Prof. Evelien Brouwer** (Associate Professor, Vrije Universiteit Amsterdam), **Prof. Benoit Dupont** (Professor of Criminology at the Université de Montréal) and **Prof. Elspeth Guild** (Senior Associate Research Fellow at CEPS) who provided comments on an earlier draft. Any errors or omissions are the sole responsibility of the authors.

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
European Parliament, manuscript completed in October 2015.

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

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.

CONTENTS

LIST OF ABBREVIATIONS

ASEAN	Association of Southeast Asian Nations
ATM	Automated Teller Machine
AU	African Union
CAM	Child Abuse Material
CEPOL	European Police College
CERT-EU	EU Computer Emergency Response Team
CIT	Cybercrime Intelligence Team
CJEU	Court of Justice of the European Union
CNP	Card-not-Present
CoE	Council of Europe
COSI	Standing Committee on Operational Cooperation on Internal Security
CTB Locker	Curve Tor Bitcoin Locker
DDoS	Distributed Denial of Service
DEA	Drug Enforcement Agency of USA
EBA	European Banking Association
EC	European Commission
EC3	European Cybercrime Centre
ECB	European Central Bank
ECI	European Critical Infrastructure
ECTEG	European Cybercrime Training and Education Group
EDA	European Defence Agency
EDPS	European Data Protection Supervisor
EFC	European Financial Coalition
EIO	European Investigation Order
ENISA	European Union Agency for Network and Information Security
EP	European Parliament
EU IRU	EU Internet Referral Unit
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
ICANN	Internet Corporation for Assigned Names and Numbers
ICROS	Internet Crime Reporting Online System
iOCTA	Internet Organised Crime Threat Assessment
ISEC	EC funding programme on the Prevention of and Fight against Crime
ISF	Internal Security Fund
ISS	Internal Security Strategy
J-CAT	Joint Cybercrime Action Taskforce
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
NATO	North Atlantic Treaty Organization
NCA	National Competent Authority
NCU	National Cyber Crime Unit
NGOs	Non-Governmental Organisations
NIS(Directive)	Directive on Network and Information Security
NSA	National Security Agency
OAS	Organisation of American States

OCTA	Organised Crime Threat Assessment
OECD	Organisation for Economic Co-operation and Development,
OSCE	Organisation for Security and Co-operation in Europe
P2P	Peer-to-Peer
PoS	Points of Sale
RATs	Remote Access Tools
RSA	Ron *Rivest*, Adi *Shamir*, and Leonard *Adleman* Algorithm
SEPA	Single Euro Payment Area
T-CY	CoE Standing Cybercrime Convention Treaty Committee
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Programme
TOR	The Onion Router
UN	United Nations
VCs	Virtual Currencies

EXECUTIVE SUMMARY

Cybercrime has become one of the key priorities for EU law enforcement agencies, as demonstrated by the establishment of the European Cybercrime Centre (EC3) in January 2013 and the development of specific European threat assessment reports in this field. High-profile criminal investigations such as the 'Silk Road' case, major data breaches or particularly nefarious hacks or malware attacks have been very much in the spotlight and widely reported in the media, prompting discussions and debates among policymakers and in law enforcement circles. Over the last few months, the cybercrime debate has specifically evolved around the issue of encryption and anonymisation.

In this context, this Study argues that debates on the law enforcement challenge of cybercrime in the EU should steer clear both of doomsday scenarios that overstate the problem and scepticism that understates it, and that **the key cybercrime concern for law enforcement is legal in nature rather than simply technical and technological**. Indeed, the Study finds that the key challenge for law enforcement is **the lack of an effective legal framework for operational activities that guarantees the fundamental rights principles enshrined in EU primary and secondary law**.

In order to address this core argument, this Study starts by analysing claims and controversies over the Internet 'going dark' on law enforcement (Section 2). It shows that these claims have been made for quite some time and should be considered as moral panics rather than accurate reflections of the challenges posed by cybercrime to law enforcement. Moreover, current controversies rehash older ones, conflating law enforcement concerns with intelligence-gathering and surveillance concerns. **Without denying the fact that criminal activities do take place online, pose technical difficulties to law enforcement services and require the availability of specific capabilities, this section demonstrates that these difficulties do not impede criminal investigation to such an extent that exceptional means should be envisaged**. While these technical aspects need to be considered, they raise issues related to policy and law rather than technology as such. The policy and law-related challenges are made greater by the fact that defining cybercrime is not an easy task. Very broad definitions have been adopted at the EU level, often leading to overlapping and sometimes conflicting mandates.

Section 3 thus analyses the institutional architecture of EU cybercrime policy. It shows that the complexity of cybercrime measures and the expansive mandates and number of actors involved in their implementation **make it difficult to ascertain and circumscribe the full scope of EU cybercrime policy**. Whereas the Council of Europe (CoE) sought to codify cybercrime powers into an international convention, much of the EU's policy to fight cybercrime is based on non-legislative measures, including operational cooperation and ad hoc public-private partnerships. Furthermore, important distinctions and restrictions designed to ensure a 'separation of powers' between state agencies concerned with law enforcement (cyber-policing), civil protection (cybersecurity), national security (cyber-espionage) and military force (offensive cyber capabilities) are harder to distinguish in the area of cybercrime, at both national and EU level. Section 3 underlines that, **within this complex architecture,** and with the blurring of the boundaries between those responsible for policing the Internet, for gathering intelligence from it, for conducting cyber-espionage against foreign targets, and for ensuring the safety of critical internet infrastructure, **the European Parliament and civil society are largely excluded from policy**

development, impeding public scrutiny and accountability. This compounds the EP's existing problems in ensuring that fundamental rights and data protection are diligently protected in the area of justice and home affairs.

In light of these gaps in oversight and accountability, Section 4 analyses in particular the challenge of jurisdiction, cooperation and fundamental rights safeguards. This section argues that **operational challenges in cybercrime law enforcement do not change the obligation of EU institutions and Member States to ensure the safeguarding of EU fundamental rights** in any operating framework of internal or transnational cooperation in law enforcement and criminal justice. Cybercrime law enforcement frequently cites the challenge of accessing and transferring data through existing Mutual Legal Assistance agreements. Yet practices taken outside of established legal channels cannot guarantee rights protections and run the risk of raising mistrust in the general public, the private sector and in transatlantic relations. Furthermore, across the spectrum of cybercrime prevention, investigation, and prosecution, the particular geography of the digital environment is said to complicate the traditional territorial foundations of law. Law enforcement bodies make continuous reference to the ways in which traditional legal structures stand in the way of operations. However, an updated legal framework designed to overcome these challenges should foreground fundamental rights concerns, **which are essential to ensure due process and a necessary condition for the successful prosecution of cybercriminal offences**.

In light of these findings, the Study concludes with key recommendations for the European Parliament. In particular, to ensure that the Parliament is not marginalised altogether with respect to the implementation and review of EU cybercrime policies by the exercise of delegated powers, EU agency discretion and non-legislative decision-making bodies, **further monitoring of EU council structures, Europol and international cooperation agreements is required** (Recommendation 1). Moreover, the EP should ensure that **the development of any cooperation/information-sharing framework guarantees the respect of fundamental rights** (Recommendation 2). In light of the current discussions on a revised CoE Cybercrime Convention, the European Parliament should, further, ensure that **the Convention's obligations are consistent with EU law and fundamental rights protections** (Recommendation 3). The EP must also ensure that cybercrime is not used as a justification to **undermine new information security protocols and the right to privacy in telecommunications, both of which are fundamental components of the functioning of the Internet** (Recommendation 4). Finally, if European law enforcement agencies need to keep pace with technological change, it is imperative that **training courses on cybercrime forensics and digital evidence include an applied fundamental rights component** (Recommendation 5).

1. INTRODUCTION

1.1. Background and Argument

In her remarks to the new Committee on Civil Liberties, Justice and Home Affairs (LIBE) on 3 September 2014, the then-Commissioner for Home Affairs Cecilia Malmström presented cybercrime as 'one of the big security issues' of her term in office, outlining the adoption of legislation on large-scale attacks on information systems and the establishment of the European Cybercrime Centre (EC3) at Europol as some of the key achievements of the European Union in this regard.[1] The Commissioner's remarks reflect the fact that cybercrime has been very much in the spotlight for policymakers as well as the general public for several years now, in Europe and elsewhere, due, in particular, to high-profile criminal investigations and convictions such as the 'Silk Road' case.[2] The European Commission's communication on the European Agenda on Security thus elevates cybercrime to one of the three key areas of concern for EU security policies.[3]

Heightened public and policy attention to the challenges posed by cybercriminal activities also means that major data breaches or particularly nefarious hacks or malware attacks receive increasing and intensive reporting. Similarly, controversies over what should be done in the area of law enforcement and cybercrime have become increasingly visible in the technology as well as mainstream media. **Over the last few months, a number of political leaders and senior security service officials have focussed the cybercrime debate around the issue of encryption and anonymisation**, arguing that technical possibilities such as the Tor software and network for anonymous online communication and virtual currency schemes, such as Bitcoin, are a challenge to law enforcement agencies and bodies, which might result in them 'going dark'. As Federal Bureau of Investigation (FBI) Director James Comey recently stated: 'Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority'.[4]

Examining the law enforcement challenges of cybercrime is timely for at least two reasons. Proposed in February 2013, the EU Directive on Network and Information Security is still under negotiation. Furthermore, the European Parliament is currently awaiting the Council's first reading position on the proposal for a new Europol Regulation, which would enable the EU Agency for Law Enforcement Cooperation and Training (Europol) to further develop its European Cybercrime Centre (EC3) with increased resources.[5]

[1] European Parliament (2014), Committee on Civil Liberties, Justice and Home Affairs Meeting, 3-4 September, Brussels, LIBE(2014) 0903.

[2] Silk Road provided an online anonymous transaction platform for the selling and buying of drugs. As widely reported in the technical and non-technical media, the platform was located in the so-called Deep Web or 'dark net' and was operated on the Tor network. Silk Road is understood to have opened in February 2011 and was shut down following the October 2013 arrest of alleged founder and owner Ross Ulbricht in San Francisco by the Federal Bureau of Investigation. In May 2015 Ulbricht was sentenced to life in prison for his role in creating and running Silk Road.

[3] European Commission (2015), The European Agenda on Security, Brussels, COM(2015) 185 final, 28 April.

[4] J. Comey (2014), *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* (Washington, D.C.: Brookings Institution), 16 October, at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (accessed July 2015).

[5] European Commission (2013), 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. Brussels, COM (2013) 173 final, 27 March.

In this context, this Study argues that **debates on the law enforcement challenges of cybercrime in the EU should steer clear of both exaggerating and downplaying the scale of the problem**. Criminal activities certainly take place online, involving the use of modern technologies. Yet such a prominent place in the discussion should not be given to the issue of encryption and the prospect of law enforcement 'going dark'. The natural corollary to claims that law enforcement is 'going dark' is to press for bulk online surveillance and communications interceptions, which have been found to be in contravention of EU law and principles by the European Court of Justice in its Digital Rights Ireland judgement on the Data Retention Directive and by the European Parliament (EP) in its inquiry on the revelations of Edward Snowden. That this discussion is even taking place, in fact, suggests that there is some confusion about the scope of EU cybercrime measures, particularly the distinction between, on the one hand, criminal investigation, and, on the other hand, cyber-intelligence, cyber-defence and online surveillance. In other words, **the key cybercrime concern for law enforcement is legal rather than simply technical and technological.** The most prominent cybercrime challenges for law enforcement identified and discussed in this Study thus involve:

- providing clarity and certainty as to the scope of EU measures in these matters;

- placing individuals at the heart of law enforcement and cybercrime discussions, not only as potential or actual victims of crime or passive recipients of protection from states or technology companies but as holders of fundamental rights and freedoms and active participants in their own protection.

1.2. Structure and Methodology

To address this core argument, this Study raises and addresses three sets of questions, in the following order:

Section 2 analyses the main claims found in the public and policy debates on law enforcement and cybercrime. Three particular aspects are discussed: the claims and controversies over the Internet 'going dark', the technical aspects of these claims and controversies, and the difficulty of defining cybercriminal activities. **Section 3** then raises the question of the aims, purposes and objectives of EU law enforcement measures in the field of cybercrime. This is an important discussion since EU action in this area involves extensive mandates, multiple actors and mostly non-legislative measures. The section analyses the institutional architecture of EU cybercrime policy and details the legal, policy and political framework and operational activities conducted under the auspices of the EU. It highlights specific challenges related to EU policy, including the complexity of EU cybercrime measures that undermine accountability and the role of the EP in this field. **Section 4** then analyses in greater depth the operational challenges of cybercrime investigations and the related challenges of transnational cooperation and fundamental rights for law enforcement. This section argues that operational challenges in cybercrime law enforcement do not change the obligation of EU institutions and Member States to safeguard EU fundamental rights in any operating framework of internal or transnational cooperation in law enforcement and criminal justice. The concluding section (**Section 5**) presents some key recommendations for the EP in light of these findings.

This Study is based on an actor-centred, multidisciplinary methodology that triangulates across a variety of legal, policy and stakeholder sources. It focusses on how law enforcement stakeholders define and view the challenges of cybercrime, and how these challenges relate to the broad policy and political objectives outlined in EU policy and legal documents, and to the available evidence on cybercriminal activities. Semi-structured interviews with various stakeholders have been conducted, in particular with the EC3 team.[6] In order to guarantee a coherent and high-level academic analysis, an advisory board of experts reviewed the academic quality and policy relevance of the Study.[7]

[6] See Annex: List of Interviews.

[7] The Advisory Board consisted of Prof. Evelien Brouwer, Prof. Benoît Dupont and Prof. Elspeth Guild.

2. SCOPING THE CHALLENGE: MORAL PANICS AND DIFFICULTIES OF LOCATING CYBERCRIME

KEY FINDINGS

- There are considerable disagreements over the definition of cybercrime, which has implications for defining and discussing the challenges posed by cybercrime to law enforcement.
- Cybercrime activities certainly present a challenge for law enforcement. However, the use of encryption and anonymisation techniques does not impede criminal investigation.
- If access to information stored on computers or communicated online has become a new target for criminal activity, it has also provided new means for law enforcement to prevent such activity as well as to solve crimes.
- Claims and controversies over the Internet 'going dark' on law enforcement rehash older ones, conflating law enforcement concerns with intelligence-gathering and surveillance concerns.

This section analyses the main claims in public and policy debates concerning law enforcement and cybercrime. Three aspects are discussed: the claims and controversies over the Internet 'going dark' (2.1), the technical aspects of these claims and controversies (2.2), and the difficulty of defining cybercriminal activities (2.3).

2.1. Moral panics and longstanding controversies over law enforcement and cybercrime

A number of political leaders and high-profile security service officials have in recent months made public interventions and statements about the relevant policy concerns raised by cybercrime. These have followed on from comments made by FBI Director James Comey about the technical possibilities of encrypting and anonymising online activities and interactions and his claim that such possibilities would prevent law enforcement services from doing their work. Speaking at the Royal United Services Institute a day after the January 2015 Charlie Hebdo attack, the Director General of MI5 echoed Comey's words, stating that '[t]he dark places from where those who wish us harm can plot and plan are increasing' and that security services 'need to be able to access communications and obtain relevant data on those people when we have good reasons to do so'.[8] A few days later, after attending the rally organised in reaction to the Paris attacks, UK Prime Minister David Cameron stressed that '[i]n extremis, it has been possible to read someone's letter, to listen to someone's call, to mobile communications [...] The question remains: are we going to allow a means of communications where it simply is not possible to do that? My answer

[8] A. Parker (2015), 'Terrorism, Technology and Accountability', speech at Royal United Services Institute, London, 8 January.

to that question is: no, we must not'.[9] Two months later Europol Director Rob Wainwright furthered this line of argument on British radio by noting that encrypted products, including ones provided by major technology companies such as Apple or Google, had 'become perhaps the biggest problem for the police and the security services authorities in dealing with the threats from terrorism' and 'changed the very nature of counter-terrorist work from one that has been traditionally reliant on having good monitoring capability of communications to one that essentially doesn't provide that any more'.[10] In a subsequent editorial published in the *Financial Times*, this view is expressed in a different way, highlighting clearly that encryption should not be banned and that there were 'serious downsides' to giving governmental authorities the kind of backdoor access into encrypted systems advocated by some in the US and Europe.[11]

These statements, in turn, elicited a strong reaction from US-based non-governmental organisations (NGOs), technology companies, trade associations and information technology security and policy experts, who penned a letter urging US President Barack Obama to 'reject any proposal that US companies deliberately weaken the security of their products'.[12] 'Strong encryption', the letter goes on to argue, 'is the cornerstone of the modern information economy's security'. Looking specifically at the question of encryption, a group comprising some of the most internationally respected computer security experts and scholars has recently suggested that part of the problem with these unfolding controversies is that 'concrete technical requirements, which industry, academics and the public can analyse for technical weaknesses and for hidden costs' have not yet been made clear.[13]

While the tensions in the current public and political debate over encryption and anonymisation may focus on technical and technological matters, a much more fundamental discussion is needed. The first observation is that these tensions initially originate in the US, which raises questions as to whether the EU is simply a follower with little capacity for an autonomous discussion over these matters. These tensions, more importantly, suggest that **the distinction between the investigation of cybercriminal activities, on the one hand, and online intelligence gathering and surveillance, on the other, has not yet been sufficiently established**. It is worth stressing that the stronger encryption products criticised by some political leaders and law enforcement officials were introduced by technology companies in the wake of the 'Snowden affair' and the debates it raised over the bulk surveillance activities of US and European intelligence services. In the past few months, moreover, some of the very security features that are currently being criticised have been shown to display severe vulnerabilities. In May 2015, for instance, a group of researchers publicised the 'Logjam attack', a series of weaknesses in a cryptographic algorithm (Diffie-Hellman key exchange) essential to widespread secure communication protocols such as HTTPS, SMTPS or IMAPS.[14] That some among the political leaders and high level officials involved in the debate over encryption and anonymisation

[9] 'David Cameron pledges anti-terror law for Internet after Paris attacks', *The Guardian*, 12 January 2015, at http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg (accessed July 2015).

[10] 'Europol chief warns on computer encryption', *BBC*, 29 March 2015, at http://www.bbc.com/news/technology-32087919 (accessed July 2015).

[11] R. Wainwright (2015), 'The Internet's corners cannot be without laws', *Financial Times*, 23 April, at http://www.ft.com/cms/s/0/e484b71e-e298-11e4-aa1d-00144feab7de.html (accessed September 2015).

[12] Letter to President Obama, 19 May 2015, at https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf (accessed July 2015).

[13] H. Abelson et al. (2015), *Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Cambridge, MA: Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report, No. 26, 6 July.

[14] D. Adrian et al. (2015), 'Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice,' 20 May, at https://weakdh.org/imperfect-forward-secrecy.pdf.

raise concerns over terrorism rather than organised crime, or speak on behalf of intelligence services, suggests that the issue of cybercrime is used in part to retain the possibility of conducting bulk communications interceptions and online surveillance. While the Europol Director suggests in the abovementioned *Financial Times* editorial that discussions about the 'dark corners' of the Internet are 'not really about privacy', it can also be argued that ultimately the stakes in the on-going discussion are also not really about technology but about fundamental questions of policy and law.

The academic literature on cybercrime suggests that these tensions are **akin to 'moral panics' rather than reasoned discussions, whose spread is facilitated by the diversity and fluidity of the concerns we regroup under the notion of cybercrime.** In criminological research, a moral panic is defined as a 'disproportional and hostile social reaction to a condition, person or group defined as a threat to societal values, involving stereotypical media representations and leading to demands for greater social control as well as creating a spiral of reaction'[15]**.** Overcoming these moral panics and clarifying the current controversies over law enforcement and cybercrime requires putting them in a historical perspective. Such an exercise is not simply academic but serves to show that the **confusion between matters of criminal investigation and criminal justice, on the one hand, and intelligence and surveillance, on the other, is not only longstanding but also foundational in efforts to determine the scope of law enforcement challenges raised by cybercrime**. In dealing with cybercrime, more precisely, as discussed in a previous Study on behalf of the LIBE Committee, law enforcement authorities compete with other security actors interested in securing 'cyber' infrastructure or in intelligence and surveillance.[16] In this regard, it is **notable that during the meetings with both Eurojust and Europol organised for this Study, neither of the agencies argued in favour of breaking down encryption, which was for both agencies considered a fundamental component of the Internet's functioning**.

In the early days of the development of the commercial Internet in the 1990s, many concerns were raised about the limits, due to technological developments, on the capacity of law enforcement and security services to investigate and monitor online activities. This was particularly the case for cryptography, and although at the time both the US and the EU were key players in the development of encryption software, it was in the US that these

[15] As defined in E. MacLaughlin and J. Muncie (2013), *The SAGE Dictionary of Criminology*, London: SAGE, 271); see also: R. Broadhurst, P. Grabosky, M. Alazab, B. Bouhours, and S. Chon (2014), 'Organizations and Cybercrime: An Analysis of the Nature of Groups Engaged in Cybercrime', *International Journal of Cyber Criminology*, 8(1), 1-20. Interest in the notion of moral panic initially arose among students of deviance who were interested in making sense of the media-intensive concern with the 'youth problem' in the late sixties and seventies (see S. Cohen (2002) [1972] *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, London: Routledge, 3rd edition). The concept proved contentious in several ways and has been intensely discussed since its introduction in criminology studies, in particular because the act of calling reactions to a specific phenomenon or behaviour a moral panic was seen as a moral stance in itself and as passing judgement (rather than analysing) the actual scope of this phenomenon. In a later edition of his seminal book, the scholar who introduced the notion returned to this matter, pointing out that calling a particular process a moral panic does not entail denying the existence of the phenomenon it relates to in the first place or attributing its unfolding to irrationality or hysteria (Cohen, *Folk Devils and Moral Panics*, viii). Raising questions in terms of moral panics, however, is not '"about" specific activities – real or imagined – or social categories, as they are about the fear and concern about, and the perceived threat from, those activities and categories' (E. Goode and N. Ben-Yehuda (2009) [1994], *Moral Panics: The Social Construction of Deviance*, Oxford: Wiley-Blackwell, 17). Examining an occurrence in terms of moral panics is therefore a way to study how the scale, nature and intensity of this occurrence is subject to contention and disagreement. For further discussion on the case of computer-related activities and behaviours, see the seminal piece R. Hollinger and L. Lonn (1988), 'The Process of Criminalization: The Case of Computer Crime Laws', *Criminology*, 26(1), 101-126; for a more contemporary discussion on identity theft, see S. Cole, A. Pontell, and D. Henry (2006), '"Don't Be Low Hanging Fruit": Identity Theft as Moral Panic', in T. Monahan (ed.), *Surveillance and Security: Technological Politics and Power in Everyday Life,* London: Routledge, 125-148.

[16] See D. Bigo et al (2012), *Fighting cyber crime and protecting privacy in the cloud*, Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), PE 462.509, Brussels.

concerns resulted in a very public controversy, known colloquially as the 'crypto wars'. Part of the reason for this controversy involved the development of decentralised, user-centric cryptographic tools.

During most of the Cold War, cryptography was a governmental matter in the US, a monopoly under the control of the National Security Agency (NSA): 'while a small market existed for unclassified commercial cryptography, the most advanced cryptographic techniques were classified and [...] limited largely to military, diplomatic and intelligence use'.[17] The government monopoly over cryptography included strong export controls, whereby the NSA also played a role in advising the State Department and the Department of Commerce on granting export licences for encryption products. The NSA also controlled the development of encryption products for commercial purposes and academic research in these areas. In 1975, for instance, the NSA famously requested the National Bureau of Standards, which was involved in developing, with IBM, a Data Encryption Standard (DES) for use in the banking and finance sectors, to weaken its DES encryption key length from 128 to 56 bits (the longer the key, the stronger the encryption).[18] That same year, Stanford University researchers Whitfield Diffie and Martin Hellman outlined **a radically new approach to encryption, public-key cryptography, which remains today a fundamental component in ensuring the safety of online activities**. Not only did Diffie and Hellman develop this approach outside of government-supervised research, but their scheme also entrusted encryption tools to users rather than a centralised authority, as had been the case until then. In public-key cryptography, every user has two keys, one publicly available to all and the other private. Communications are encrypted using the public key but can only be decrypted using the private one. The set of algorithms that later implemented the Diffie-Hellman concept, known as RSA (after the initials of the three MIT scientists who developed and later commercialised them), was considered stronger than DES (because longer encryption keys are used). RSA was initially considered by the NSA a threat to national security.[19]

Controversies over the individual and commercial use of encryption in relation to security concerns resurfaced in the 1990s due to a second technological breakthrough, a software programme called PGP (for 'Pretty Good Privacy') developed by Philip Zimmermann. PGP purported to implement the RSA algorithms on personal computers and was released in 1991 as freeware.[20] While PGP was initially circulated on a material support (diskettes), it was soon posted on the online discussion system USENET. In 1993, the Department of Justice (DoJ) opened an investigation into Zimmermann for possibly violating US export control laws on encryption products.[21] The investigation was closed in 1996 without any charges being filed against Zimmermann. Meanwhile, from 1993 onwards, officials from the Clinton administration started considering alternatives for dealing with the issue of law enforcement access to encrypted electronic communications. If doing nothing was seen to jeopardise law enforcement wiretapping powers, national security and foreign policy, weak encryption was considered too much of a risk, particularly for commercial applications: in the end the course of action chosen was to combine strong encryption with exceptional

[17] K. W. Dam and H. S. Lin (eds.) (1996), *Cryptography's Role in Securing the Information Society*, Washington, D.C.: National Academies Press, 414.

[18] Ibid., 417. The involvement of the NSA would remain significant in later years, including after the adoption of the 1987 Computer Security Act that gave the National Institute of Standards and Technology (successor to the NBS) responsibility for the development of standards and the evaluation of cryptographic products for non-classified applications.

[19] G. Giacomello (2002), *National Governments and Control of the Internet: A Digital Challenge*, London: Routledge, 42.

[20] S. Levy (1993), 'Crypto Rebels', *Wired Magazine*, 1(2), May/June, at http://archive.wired.com/wired/archive/1.02/crypto.rebels_pr.html (accessed July 2015)

[21] Dam and Lin, *Cryptography's Role in Securing the Information Society*, 164.

access. This option became known as 'escrowed encryption'.[22] The 'Clipper chip' scheme was based on a unique secret key or master key that would be embedded in the chips of electronic devices. The secret key would be split into two components, held in escrow by a trusted third party. The combination of chip-unique key and escrow system would enable law enforcement authorities to identify a specific device of interest, request its components from the two trusted third parties (in this case, US government agencies) and decrypt communications.[23] Scientific research into the Clipper chip initiative eventually showed that escrow key or key recovery schemes were too technically difficult to implement, too costly, and too much of a security risk given the requirement that the master key or its components had to be stored in specific locations where they could be retrieved.[24] These findings, together with resistance from technology companies due to costs, led to the abandonment of the Clipper chip and other escrow key-based schemes in the second half of the 1990s.

The history of the 'crypto wars' is critical when examining the area of law enforcement and cybercrime today, including in the context of EU policy. The controversies that unfolded over encryption from the 1970s to the end of the 1990s contributed significantly to shaping the landscape of today's Internet. They indicate that **worries over the Internet 'going dark' on law enforcement primarily concern intelligence and security services, which focus on bulk data collection and surveillance**. Current debates replay these initial controversies and the conflation between the concerns of law enforcement authorities and those of intelligence services.

2.2. Is there a 'cyber-arms race'? Technical aspects of law enforcement and cybercrime

The label of cybercrime covers a broad range of activities, often described in very technical terms. The following paragraphs provide some examples of these activities, including data breaches, network attacks, malware, darknets and criminal financial operations.[25]

Data breaches are possibly the most basic activity covered by the label of cybercrime, even though they can be motivated by other factors. They refer to the illegal intrusion into the database of an institution, in order to acquire data that is generally confidential or sensitive. Data breaches can be politically motivated (in which cases the label of cybercrime is heavily contested). The most famous such breaches have been the retrieval of State Department cables by Bradley/Chelsea Manning, published by Wikileaks in 2013; and the retrieval of classified US intelligence documents by Edward Snowden, publicised in the summer of 2014. Data breaches can also be carried out for purposes of espionage. The most important recent data breach is probably the acquisition of 21.5 million records held in the US Office of Personnel Management, possibly by a foreign power.[26] The data is likely to be matched with other databases, such as credit history, social media or medical databases in order to find vulnerable targets with security clearances within the US system. Finally, data breaches can be of a criminal nature, where

[22] Ibid., 170.
[23] Ibid., 171.
[24] H. Abelson et al. (1997), 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption', New York, NY: Columbia University Academic Commons, at http://hdl.handle.net/10022/AC:P:9130 (accessed July 2015).
[25] These examples draw on some of the main issues raised in the latest issue of EUROPOL's IOCTA report. Europol (2015), *The Internet Organised Crime Threat Assessment (iOCTA)*, The Hague: Europol, 18-57.
[26] M. Hosenball (2015, July 14), 'U.S. has yet to notify 21.5 million data breach victims: officials', at http://www.reuters.com/article/2015/07/14/us-cybersecurity-usa-notification-idUSKCN0PO2SE20150714 (accessed October 2015)

the objective is to acquire information that can be sold, or used to carry out fraudulent activities such as blackmailing, credit card fraud or identity theft. Several companies have been victims of data breaches. The most recent has been the widely reported attack on dating website Ashley Madison.[27] Other breaches include Talk talk, AdultFriendFinder, the World Trade Organization and British Airways.[28]

Network attacks involve illegally denying network access to a specific server. The most common and simple attack is the Distributed Denial of Service (DDoS) attack, which uses a network of computers (also called *botnet*) in order to flood a specified server with requests, resulting in its inaccessibility to other users. DDoS attacks, like data breaches, can be motivated by different factors. Recently, Europol documents the practices of a group identified as DD4BC (DDoS for Bitcoin) which threatens companies or institutions with DDoS attacks, and asks for payment in bitcoin not to carry it out.[29]

Malware can be broadly defined as any piece of software that is designed to damage or perform unwanted actions on a computer system.[30] Forms of malware include viruses and worms (aimed at damaging or erasing content), as well as Trojan horses and spyware (aimed at taking control of the computer and/or sending information to a third party without the knowledge of the computer owner). Europol identifies three specific types of malware as “key threats”:

- The first is ransomware. For example, Trojan horse software like Cryptolocker, running on Microsoft Windows, emerged in September 2013. Propagated via email, once installed it encrypts certain files using RSA public-key cryptography. The software then asks the computer owner to pay a certain amount of money to an anonymous bitcoin account in order to decrypt the files. Even if the malware can be easily removed, the files remain encrypted if the ransom is not paid. CryptoLocker was defeated in May 2014 via Operation Tovar[31], during which the list of private keys needed to decrypt ‘ransomed’ files was recovered. Other ransomware examples include Reveton, CTB-Locker, TorrentLocker and Cryptowall.

- Trojan horses or Remote Access Tools (RATs) are pieces of software designed to access without authorisation key pieces of remote software or hardware (e.g. microphones, webcams, keystrokes on the keyboard, installing or uninstalling applications, etc.). The most famous of such Trojan horses was the Blackshades trojan. The Trojan installed itself on victims’ computers via webpages, or infected external storage devices such as USB drives. Once the device was infected, the software allowed its users to control remotely the victims’ keystrokes (in order to recover passwords for example), webcam and microphone. Additionally, it included the victim’s computer in a botnet (a network of unwilling remote-controlled computers), so that it could be used as a proxy server to perform, for example, DDoS attacks. Blackshades was defeated in 2014 in an investigation led by the FBI in which Eurojust and Europol actively took part.[32] Other notorious Trojans include Netbus, Sub7, Back Orifice, Beast, Zero Access, Koobface, Vundo.

[27] BBC Report (August 2015), ‘Ashley Madison: Who are the hackers behind the attack?’ at: http://www.bbc.co.uk/news/technology-34002053 (accessed October 2015).

[28] Europol (2015), p. 41.

[29] Ibid.

[30] P. Christensson (2006), ‘Malware Definition’, *Tech Terms*. Sharpened Productions. At http://techterms.com/definition/malware (accessed October 2015).

[31] D. Storm (2014), ‘Wham bam: Global Operation Tovar whacks CryptoLocker ransomware & GameOver Zeus botnet’, at http://www.computerworld.com/article/2476366/cybercrime-hacking/wham-bam--global-operation-tovar-whacks-cryptolocker-ransomware---gameover-zeus-b.html (accessed October 2015).

[32] FBI report (May 2014), ‘Coordinated Law Enforcement Actions Announced’, at : https://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown (accessed October 2015) and EUROJUST report (October 2014), ‘International operation hits BlackShades users’, at : http://www.eurojust.europa.eu/press/pressreleases/pages/2014/2014-05-19.aspx (accessed October 2015).

- An overlapping category, also part of the Trojan horse family of malware is, in Europol parlance, "info stealers". These are pieces of software primarily designed to steal information or data stored on a victim's computer. The trojan "Zeus" is one such example. Created in 2006 it became mainstream in 2009, when it affected institutions such as Bank of America, NASA, ABC, Oracle, Cisco and Amazon[33]. Its main functionality is known as "man-in-the-browser" keystroke logging and form grabbing. The software evolved in 2010, when the main developer gave access to the source code to other developers. It has since evolved into other Trojans such as Gameover Zeus (GOZ) or P2P Zeus. Other such pieces of software include Citadel, Ice IX, Spyeye, Dridex, Dyre, Tinba, Carberp, Torpig, Shylock.

Another main issue of concern is darknets. In very simple terms, a darknet is a network built on top of another network (also known as overlay network), which can only be accessed through a specific connection protocol (either via a specific software configuration, or access codes for example). Peer-to-peer (P2P) networks (such as the ones established via torrent file sharing) are an example of such darknets: they use the regular Internet network to build an additional layer of exclusivity and privacy. Another well-known darknet is The Onion Router (TOR) network. While TOR was developed in great part by the US authorities, in the US Naval Research Laboratory and then within DARPA, in order to support free-speech activists across the globe, it has also been used to conduct illegal activities. **A good example of the use of TOR to conduct illegal activities is the Silk Road case.** Silk Road was a webpage[34] launched in 2011. It hosted a black market that guaranteed the anonymity of buyers and sellers. Any type of illegal goods or services could be purchased on the website, from illegal drugs to fake driving licences and guns. It is estimated that USD 15 million worth of transactions took place annually on the website, all paid in Bitcoin (the specific issue of Bitcoin is developed in Section 3). On 2 October 2013, the FBI arrested Ross William Ulbricht and accused him of running the website. On May 29, 2015, Ulbricht was sentenced to life imprisonment. In November 2014, 21 countries (including EU Member States and the US) participated in Operation Onymous, targeting successor darknet marketplaces such as Silk Road 2.0, Cloud 9 and Hydra. Twenty-seven websites were shut down in total.

Another type of activity made possible by darknets is Child Sexual Exploitation. P2P networks are used to exchange images and videos of child abuse material (CAM), even though high-bandwidth internet has allowed widespread live streaming of CAM, which leaves fewer traces than P2P files (the files require storage). Darknets are also used as venues for marketing such material.

Finally, payment fraud and criminal financial operations deserve mention. Credit card and payment fraud represents one of the most lucrative activities online. It is estimated that in 2013, the number of fraudulent transactions conducted within the Single Euro Payments Area (SEPA)[35] reached EUR 1.44 billion, representing approximately 3.3% of the EUR 43.6 billion worth of payments in the EU.[36] Payment fraud and criminal financial operations can take various forms:

- ATM/PoS techniques. A certain number of techniques are employed physically at the Automated Teller Machines (ATM) or at the points of sale (PoS). Skimming (copying the card information, including PIN and security code) can occur passively or

[33] ZBot data dump discovered with over 74,000 FTP credentials', *Tech Herald* (June 2009).
[34] The address looked like: http://silkroad6ownowfk.onion
[35] As of July 2015, SEPA consisted of the 28 EU member states as well as Iceland, Liechtenstein, Monaco, Norway, San Marino and Switzerland.
[36] Europol (2015), The Internet Organised Crime Threat Assessment (iOCTA), The Hague: Europol, 32.

actively with the use of dedicated fraud systems such as ATM Malware.[37] According to Europol, such activities are generally in decline in Europe.

- Card-not-present (CNP) fraud. Fraudulent transactions that do not require the physical presence of the card are estimated to represent more than two thirds of credit card fraud for operators such as Visa and Mastercard.[38] They are enabled by the wholesale exchange or resale of large databases containing credit card information – obtained through hacking or social engineering (whereby confidential or compromising information is acquired through deception or manipulation).

These examples illustrating the reliance on specific digital tools for illicit activities certainly present a technical challenge for law enforcement. However, we need to steer clear both of doomsday scenarios that overstate the problem and scepticism that understates it. Indeed, ongoing controversies about law enforcement and cybercrime often reproduce the discourse of the 'cyber-arms race': in a context of increasing volume and sophistication of cyber-attacks, governments purportedly struggle to catch up. This depiction is broadly misleading, and as has been made clear by the interviewees contacted for this research and from the available evidence, **the use of encryption and anonymisation techniques does not impede criminal investigation to such an extent that extraordinary means, such as the imposition of backdoors to encryption systems, should be made available to law enforcement. Instead, it requires the availability or development of specific technical skills**.

Current controversies about encryption and anonymisation have elicited a strong response from the scientific and technology community. Technological changes have frequently sparked claims by law enforcement agencies that they were 'going dark', as this Study has demonstrated above and as seventeen high-profile technologists recall in a 2015 report addressing governments' claims to exceptional access to all data and communication.[39] In 1992, for example, the FBI's Advanced Telephony Unit warned that within a few years it would be unable to carry out wiretaps. As the Snowden affair has revealed, however, the opposite has been true; indeed, 'law enforcement has much better and more effective surveillance capabilities now than it did then'.[40] **The claim that law enforcement agencies are playing catch-up in the 'cyber-arms' race should be seen as a staple justification used by security agencies to pursue their bureaucratic interests, chief among them an increase in budget and the use of exceptional powers**. This phenomenon has been widely documented in the security literature on the military or police.[41] In terms of IT security systems, in 1999, the discourse of security agencies around the 'Millennium Bug' (Y2K) and the requests for unnecessary funding it triggered are a good case in point.[42] The argument of the technological gap should therefore not be analysed as an objective state of affairs but rather as one argument that can be strategically used by security agencies to pursue their interests. This observation does not mean that these capabilities are justified or that their use is legitimate but that **the notion of a 'cyber**

[37] For more on these techniques, see Europol 2015, p. 33.

[38] Ibid.

[39] Abelson et al., *Keys under Doormats*.

[40] Ibid., 1.

[41] On the military, see G. T. Allison (1971), *Essence of Decision: Explaining the Cuban Missile Crisis*, Boston: Little Brown; and R. K. Herrmann and R. N. Lebow (2004), *Ending the Cold War: Interpretations, Causation, and the Study of International Relations*, Basingstoke: Palgrave Macmillan. On the police, see D. Bigo (1996), *Polices en réseaux: L'Expérience européenne*, Paris: Presses de la Fondation Nationale des Sciences Politique; M. Anderson et al. (1996), *Policing the European Union*, Oxford: Oxford University Press; and M. Den Boer (1998), 'Wearing the Inside Out: European Police Cooperation Between Internal and External Security', *European Foreign Affairs Review*, 2(4), 491–508.

[42] D. Bigo (2010), 'Freedom and Speed in Enlarged Borderzones', in V. Squire (ed.), *The Contested Politics of Mobility: Borderzones and Irregularity*, London: Routledge.

arms race' where security services are falling behind cyber-wrongdoers should be nuanced at the very least.

The invention and commercialisation of the Internet have meant that our daily lives are increasingly reliant on the ability to safely store and communicate information via computers. **Access to information stored on computers or communicated online has therefore become a new target for criminal activity, but it has also provided a new means for law enforcement to prevent such activity as well as to solve crimes**. As one journalist suggests, contemporary transformations in information technology are framed in ways that recall earlier transformations in transportation: the invention of the modern automobile opened up new possibilities for faster getaways for bank robbers but also enabled the police to receive the same, if not faster, cars.[43]

The technical challenges cybercrime poses to law enforcement should be analysed against this backdrop. As a prosecutor working on cybercrime at the European level informed the authors of this report, **there are in fact few aspects of cybercrime that substantially challenge law enforcement agencies in the two main areas covered by the label 'cybercrime' - namely, (1) when a computer is the target of the crime and even more so when (2) a computer is used as a tool to commit a crime**. Qualifying the offences is not a particular problem. In the first instance, for example, hacking is indeed trespassing, cracking is burglary, website defacement is vandalism. The use of malicious code (viruses, worms, Trojan horses) falls under different categories depending on its use. When computers are used as tools (2), such as in the cases of fraud, theft, extortion, stalking, forgery or child pornography, the usual criminal procedures apply.

Some aspects of cybercrime make investigations and prosecutions more difficult - but their nature is not radically changed. The first aspect concerns the geography of the crime: it generally takes place over multiple regional or national jurisdictions, therefore requiring international collaboration (as developed in Section 4). Second, the question of scale can also lead to difficulties: when millions of records, accounts, credit cards, or personal photos are hacked, technical capacities and manpower are required to deal with the amount of information involved. A third challenge concerns the capacity for offenders to hide their identity. Here again it is mostly a question of the competence and skills of the forensic investigator to pick up the electronic traces and signatures left by wrongdoers – which is also what happens when dealing with skilful offline criminals who know how to hide their tracks, for example. **In other words, of all the difficulties law enforcement agents face when dealing with cybercrime, the two main ones are non-technical in nature.** They concern (1) the difficulties of carrying out investigations in multiple jurisdictions (regional, national, international) - addressed further in Section 4 - and (2) hiring and retaining staff that possess the technical and legal skills to carry out proper cybercrime forensic work. These are issues related to law and policy rather than technology.

Despite this conclusion, encryption of stored data and communications data has been pinpointed as an area in which policy changes could facilitate the work of law enforcement. The encryption of stored data concerns, for example, the capacity to encrypt hard drives, USB sticks or data remotely stored in a server through commercial cloud services (Dropbox, Google Drive or Microsoft Skydrive/One drive) so that only through decryption, which requires a specific key or password, can their contents be accessed and read in

[43] 'Cyber-Crime: Law Enforcement Must Keep Pace With Tech-Savvy Criminals', *Govtech.com*, at http://www.govtech.com/dc/articles/Cyber-Crime-Law-Enforcement-Must-Keep-Pace.html?page=1 (accessed July 2015).

plaintext. Similarly, the encryption of communications concerns the ability to exchange information on the web (http and https) through email, or hold conversations through services such as Skype or via text messages, with services such as Whatsapp, Facebook Messenger or Apple iMessage, without them being accessible to a third party that does not possess a decryption key. It has been argued in the public debate that such encryption tools are preventing law enforcement agencies from accessing useful documents; therefore, the argument goes, commercial software companies offering encrypted services should allow law enforcement agencies to access the stored data or the communications data in specific circumstances, within the boundaries of the law. This claim is generally referred to as 'exceptional access'.

What could such access for law enforcement agencies look like? In their 2015 paper 'Keys Under the Doormat', some of the key technologists involved in the 1990s 'crypto wars' discuss the challenges posed by existing technological possibilities.[44] For both scenarios (stored data and communications data encryption), exceptional access would require a system of additional keys (escrow keys, akin to a 'master key') stored in a secure third-party institution. Such systems already exist in the corporate world: employees of large financial institutions, for instance, generally use a computer with encrypted hard drives. If the computer needs to be inspected, either by the company staff or law enforcement, the security department is able to decrypt the computer via a system of escrow keys.

According to some of the law enforcement proposals, a similar system could be implemented for encrypted communications. Encrypted communications (such as SSL/TLS, for example, which is used when connecting to a website such as a bank or webmail through a secure https protocol) work through a similar system of encryption. Data is usually encrypted with a symmetric key (one that can be used both for one party to encrypt the data and the receiving party to decrypt the data), which is in turn encrypted via a public/private encryption system (in order to transmit safely the symmetric key from the sender to the receiver). In this second step, the entity shares a public key – which can be used for decryption only through the use of a private key – with the entity it wishes to communicate with. Law enforcement agencies generally suggest adding an escrow system during this second encryption phase: in addition to public/private key encryption, there would be an additional key accessible to the escrow agent. In other words, as for access to data stored on a laptop through a master key, there would also be a master key to communications data.[45]

While at first glance this appears to be a simple and practical solution to the problem of how to access encrypted data**, technology experts highlight three important points which indicate that the solution could create more problems than it solves if the focus of the discussion is exclusively technical**. The first concerns what in technological parlance is called the problem of 'forward secrecy'. While public/private key encryption has been the standard way of exchanging encrypted information for several years, more and more actors are moving away from it. The main problem of the public/private key system is that if the private key of an entity (say, for example, a bank) comes into the possession of a third party (a cybercriminal), all communications encrypted via the public key become vulnerable. In other words, getting hold of the private key not only compromises the intercepted communication but all past and future communications encrypted with the private key. For this reason, more and more entities are moving to a system which consists of exchanging temporary keys during any given communication

[44] Abelson et al., *Keys under Doormats*.
[45] Ibid., 11.

(session). The key is valid for a particular session and then deleted. Getting access to a session does not allow an eavesdropping third party to gain access to the other encrypted communications.[46] Thus, **the system of key escrow, based on a notion of permanent master keys, does not work with forward secrecy, since adopting the escrow system would force many companies or institutions to operate with a less secure system of public/private keys.**

The second reason concerns the issue of systems complexity. All cryptology and software developers agree that the simpler the encryption procedure or the software, the easier it is to secure against vulnerabilities. Adding a layer of master keys through a system of key escrow increases the number of vulnerabilities offered to malicious third parties. One example is that of communications authentication. The current practice of encryption generally uses authenticated encryption: not only is the data cyphered so that it prevents unwanted parties from having access to the content, but it also provides authentication, ensuring (1) that the entity at the other end of the communication is the desired party and (2) that the content has not been altered or forged. Gaining access to the key allows, therefore, not only access to its content but also makes it possible to forge traffic from one entity to another, making it look as it came from a legitimate entity. **A system of key escrow would therefore introduce a further layer of vulnerability in the encrypted data.**

The third, and possibly **most important, problem sits between the technical and governance domain; it can be summarised in a very simple question: who holds the keys to the safe?** Rather than a technical matter, this is a policy and more importantly a legal question. As we have argued, the idea of exceptional access relies on a superseded notion of permanent keys; most of the innovative encryption methods built on the principle of forward secrecy rely on discardable, temporary encryption keys. Yet if one wants to implement a system of key escrow, who will such an authority be? It is easy to believe that at the European level such lists of keys would be entrusted to national law enforcement agencies. But how would that function internationally? In light of the Snowden revelations, would French or German companies be inclined to use encryption software that US law enforcement agencies can access officially? What about software developed in countries such as China or Russia or communications between China and the UK or France: what escrow agent could both sets of governments trust?[47] **In other words, in the current state of technological development, any system of exceptional access based on the principle of key escrow opens up a Pandora's box related to governance: who would be entitled and entrusted to hold such keys?**

2.3. Debates over the definition of cybercrime

So far, this Study has shown that current controversies over law enforcement and cybercrime reiterate the conflation between concerns linked to criminal investigations and concerns linked to intelligence and surveillance. It has been further shown that the area of law enforcement and cybercrime raises questions that are ultimately issues of policy and law rather than technical or technological matters. In order to further this discussion, however, it is important to acknowledge and take into account the fact that the definition of cybercriminal activities and the examination of their effects cannot be taken for granted.

[46] Ibid., 12.

[47] Ibid., 13.

The European Commission defines cybercrime as 'criminal acts that are committed online by using electronic communications networks and information systems'.[48] Calling cybercrime 'a borderless problem', the European Commission's definition classifies cybercrime into three categories: crimes directed at elements specific to the Internet (such as information systems or websites); online fraud and forgery; and 'illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia'. Based on both its mandate and internal organisation (i.e., the Europol Focal Points that deal with 'cyber' issues), Europol's EC3 endorses in its reporting a more specific understanding by distinguishing between 'Internet-enabled crime', 'child sexual exploitation online' and 'payment card fraud'.[49] **These definitions raise a series of challenges for cybercrime law enforcement**.

There is first a question of scale. The offences listed in the second and third categories of the European Commission's definition can be considered crimes even in the absence of a 'cyber' element. For example, bank fraud, child sexual abuse or terrorism are crimes with or without the use of the Internet and occur no matter the degree of digital coordination. This definitional issue can have implications in terms of jurisdictional authority as crimes can fall under the remit of different law enforcement bodies with different capabilities and approaches. This aspect is related to the **increasing difficulty to distinguish the boundaries between cybercrime and cybersecurity,** and, more specifically, between crime, terrorism, national and international security, and infrastructure protection. One implication is that cybercrime, cybersecurity and international security concerns can become intertwined in policy and operational practice. Cybercriminal activities might be of concern to agencies and services tasked with cybersecurity or cyber-intelligence matters, but these agencies and services may not be responsible for cybercrime. For example, critical information infrastructure agencies such as the European Union Agency for Network and Information Security (ENISA) are tasked with issues of preparedness and resilience which overlap with national and EU security and defence concerns, as in the EU Cyber Defence Policy Framework adopted by the Council in 2014, which discusses the goal of developing 'possible civilian-military synergy'.[50]

The difficulty of defining cybercriminal activities and assessing their effects is a central matter in the scientific literature.[51] These debates are also relevant from a policy perspective, as they often lead to overlapping and sometimes conflicting mandates, as will be seen in the next section analysing the institutional architecture of EU cybercrime policy.

[48] European Commission Migration and Home Affairs Website, at http://tinyurl.com/mxnog29 (accessed June 2015).

[49] Europol (2014), *The Internet Organised Crime Threat Assessment (iOCTA)*, The Hague: Europol, 15.

[50] Council of the European Union (2014), EU Cyber Defence Policy Framework, Brussels 15585/14, 18 November, 9, at http://tinyurl.com/ojqum7y (accessed June 2015).

[51] See J. Lusthaus (2013), 'How Organized Is Organized Cybercrime?', *Global Crime*, 14(1), 52-60.

3. INSTITUTIONAL ARCHITECTURE OF EU CYBERCRIME POLICY

KEY FINDINGS

- The complexity of cybercrime measures and the variety of actors involved in their implementation make it difficult to ascertain and circumscribe the full scope of EU cybercrime policy.
- Much of the EU's policy on fighting cybercrime is based on non-legislative measures, which largely excludes the European Parliament and civil society from policy development.
- Important distinctions and restrictions designed to ensure a 'separation of powers' between the state agencies concerned with law enforcement, civil protection, national security and military force are harder to discern in the area of cybercrime, at both national and EU level.
- In term of prevention, there is significant overlap between the EU's critical infrastructure protection programme and EU measures to prevent cybercrime.
- Demands for new cyber-surveillance powers to combat 'encryption by default' are unworkable and undesirable. Law enforcement agencies should focus on developing the skills and expertise for cybercrime investigations while helping users of new technologies take responsibility for their own safety online.

This section examines the legal, political and institutional development of EU cybercrime policy. It is split into two broad subsections: the first charts the evolution and reach of the current EU policy framework, while the second examines the operational measures and activities devised to implement those policies. From the outset it is important to stress the complexity of EU cybercrime policy. This is partly due to the broad definition of 'cybercrime' underlined in Section 2 and the wide range of activities captured by policy and practice, the wide range of EU policy areas with a 'cyber' component, and the contradictory goals of these different 'cyber'-mandates.

The cybercrimes covered by EU law and policy include traditional crimes such as fraud or theft when they involve electronic communications systems; crimes relating to illegal content such as child pornography, incitement to terrorist acts, the glorification of violence, and racist and xenophobic material; and crimes unique to electronic networks, such as 'hacking' or illegal interference. The cross-border nature of cybercrime means that investigations and prosecutions have to overcome the barriers to cooperation imposed by diverse jurisdictional rules and legal frameworks governing the collection and use of electronic evidence.

The EU policy briefs that contain cybercrime competences and/or obligations include the Internal Security Strategy (ISS), telecommunications regulations (now part of the Digital Agenda for Europe), critical infrastructure protection (insofar as it relates to protecting designated information systems from attack), and various elements of the 'cybersecurity' agenda (which, although the subject of a separate study for the LIBE committee, are addressed below when they are closely related to the issues raised in this Study).

The links between EU cybercrime and cybersecurity policy are complicated still further by their uneasy relationship with the offensive and defensive cyber-operations of state military and security agencies, including those of EU Member States. Although the EU is now developing cyber-defence capabilities, these issues remain largely outside the scope of the European Union's competences, with recent allegations that the intelligence agencies of one Member State interfered with critical infrastructure in other Member States, demonstrating the challenges in developing credible policies in this field.[52]

3.1. Legal and political framework

3.1.1. Legal framework

The scope and complexity of EU cybercrime policy have engendered various structural tensions between policy objectives and legal obligations. EU Treaties and subsequent secondary legislation constitute a mandate for measures providing a high level of safety and protection for telecommunications systems and, more broadly, the smooth functioning of the internal market.[53] These provisions provide a legal basis for EU legislation in the areas of cybersecurity and critical infrastructure protection.[54] Combating cybercrime has also become a central objective in the construction of the EU Area of Freedom, Security and Justice.[55] Article 83 of the Treaty on the Functioning of the European Union (TFEU) provides specifically for the adoption of common rules concerning the definition of criminal offences and sanctions in the area of 'computer crime' and other serious crimes. Prompted by the CoE Convention on Cybercrime, the EU adopted a Framework Decision (now a Directive) criminalising attacks on information systems and outlining various offences falling within the scope of recognised cybercrimes (as developed further in section 3.1.5).

EU procedural law has created a cross-border framework for national and EU law enforcement agencies to prevent and respond to relevant offences. This includes the 2014 Directive on the European Investigation Order (EIO), which, when it enters into force in mid-2017, will replace many of the previous EU mutual assistance provisions, including those on intercepting communications, monitoring bank accounts and accessing

[52] In particular the allegations regarding the unlawful interference with the Belgian telecommunications operator Belgacom and the Dutch SIM card manufacturer Gemalto. See R. Gallagher (2014), 'Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco', *The Intercept*, 13 December, at https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/ (accessed July 2015); and J. Scahill and J. Begley (2015), 'The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle', *The Intercept*, 19 February, at https://firstlook.org/theintercept/2015/02/19/great-sim-heist/ (accessed July 2015).

[53] TFEU Article 114 provides for the adoption of measures to secure the smooth functioning of the internal market, including high levels of safety and protection.

[54] In line with the notion of 'service continuity', specific security and protection measures are often included in sector-specific Internal Market legislation based on TFEU Article 114, such as the 'Universal Services Directive' (Directive 2002/22/EC). TFEU Article 6(f) gives the EU the competence to 'support, coordinate or supplement' the actions of the Member States in the area of civil protection. TFEU Article 196 contains provisions for civil protection, calling on the EU to 'encourage cooperation between Member States in order to improve the effectiveness of systems for preventing and protecting against natural or man-made disasters'. This excludes 'harmonisation of the laws and regulations of the Member States' but corresponds to some of the general Critical Infrastructure Protection objectives.

[55] TFEU Article 4(2)(f).

communications data retained by service providers in other Member States, while introducing new safeguards for suspects and defendants.[56] This will set a higher standard of fundamental rights protection for intra-EU mutual existence than exists in the EU-USA Treaty on Mutual Legal Assistance (MLA) agreed in the aftermath of 9/11.[57] **While substantive and procedural criminal law measures set out in EU legislation are now subject to co-decision with the EP, most operational cooperation takes place through mechanisms and organisations that are only thinly accountable to the EP**.[58]

Any legislation and operational measures in the field of cybercrime must respect the EU Charter of Fundamental Rights and other international human rights instruments.[59] As the Commission wrote in its 2013 Communication on a Cybersecurity Strategy of the European Union: 'Increased global connectivity should not be accompanied by censorship or mass surveillance'.[60] These tensions are exacerbated by the fact that many cyber-infrastructures are privately owned and that the policing of cyberspace is, to a significant extent, both operationally unprecedented and legally unsettled, for example with respect to automated cyber-surveillance systems.

In addition to the EU Data Protection Directive and draft General Data Protection Regulation (GDPR), the 'E-privacy' Directive places additional obligations on companies in the electronic communication sector to ensure the confidentiality of communications and to prevent unauthorised access to customer data.[61] However, the recently annulled Data Retention Directive (which is still effectively in force in the majority of EU Member States), together with various EU cybercrime policies discussed in this Study, impose additional obligations on private actors who restrict the right to privacy of their customers on law enforcement grounds.[62] Similarly, where EU cybercrime legislation criminalises the publication of illegal content, service providers may be party to voluntary arrangements or subject to compulsory blocking or removal of that content, placing limits on freedom of expression. Information and communications technologies have effectively outsourced responsibility for censorship from states to companies.[63] This may be relatively uncontroversial for content related to sexual exploitation or child pornography, but it has raised concerns by human rights organisations when it comes to copyright enforcement and 'radicalising'/'terrorist' content.[64] Critics also say that the export of legitimate security tools

[56] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

[57] Agreement on mutual legal assistance between the European Union and the United States of America (OJ L 2003 181/34).

[58] TFEU Articles 71-76.

[59] This includes the European Convention on Human Rights and the International Covenant on Civil and Political Rights.

[60] European Commission (2013), Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace, Brussels, JOIN(2013) 1 final, 7 April.

[61] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; European Commission (2012), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels, COM(2012) 11 final, 25 January; and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[62] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. Annulled by Judgment in Case number C-293/12, Court of Justice of the European Union, 8 April 2014.

[63] S. J. Murdoch and R. Anderson (2007), 'Shifting Borders', *Index on Censorship*, April.

[64] See, for example, Europe Commissioner for Human Rights (2015), Positions on counter-terrorism and human rights protection, Council of Europe CommDH Position Paper (2015)1, at https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2757196&SecMode=1&DocId=2274090&Usage=2 (accessed July 2015).

may be undermined by recent EU efforts to restrict the sale to repressive and authoritarian regimes of technologies that can be used for mass surveillance, monitoring, tracking and interception.[65]

Cybercrime policy indeed raises important issues related to fundamental rights, which will be developed further in Section 4.

3.1.2. Council of Europe Cybercrime Convention

The 2001 CoE Convention on Cybercrime sought to harmonise the definition of offences committed through the Internet and other computer networks in such areas as copyright infringement, computer-related fraud, child pornography and 'hacking'.[66] It also sought to harmonise police powers and provide for cross-border assistance in such actions as searching computer networks and intercepting communications.

The Cybercrime Convention entered into force on 1 July 2004 and has to date been signed by 54 countries, 46 of whom have ratified it. Three EU Member States (Greece, Ireland and Sweden) have yet to ratify it. The Convention, which is open for worldwide accession, has been ratified by seven states from outside the Council of Europe area, including Australia and the US.[67] The Convention is supplemented by a Protocol on acts of a racist and xenophobic nature committed through computer systems, which entered into force on 1 March 2006.[68] Six EU Member States have not signed the Protocol; a further six have signed but not ratified it.[69]

The CoE Convention and its Protocol serve as a guideline for any country developing comprehensive national legislation against cybercrime. Signatories to the Convention are required to transpose a list of offences into their domestic law: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, and offences related to copyright. The additional Protocol requires signatories to criminalise the online dissemination of racist and xenophobic material, and threats and insults of a racist and xenophobic nature. States can effectively exclude offences relating to the denial of the Holocaust and other genocides and may exercise prosecutorial discretion over acts that do not intend to incite hatred, discrimination or violence.

The CoE Convention also sets out a number of procedural mechanisms including the expedited preservation of stored data, the expedited preservation and partial disclosure of traffic data, the search and seizure of computer data, the real-time collection of traffic data, and the interception of content data. The Convention also mandates states to grant law enforcement agencies the power to compel Internet Service Providers (ISPs) to retain data about their customers for law enforcement purposes ('data retention') and to monitor an individual's online activities in real time. It also contains provisions on cross-border access to data sought by investigating agencies in another country. Parties to the Convention are

[65] Commission Delegated Regulation of 22.10.2014 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items. On concerns about these measures, see Thomson, I. (2015) 'The weapons pact threatening IT security research', *The Register*, 6 June, at http://www.theregister.co.uk/2015/06/06/whats_up_with_wassenaar/ (accessed July 2015).

[66] Council of Europe Convention on Cybercrime, Budapest, 23 November 2001 (CETS No. 185).

[67] In addition to Australia and the USA, the treaty has been ratified by the Dominican Republic, Japan, Mauritius, Panama and Sri Lanka.

[68] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28 January 2003 (CETS No. 189).

[69] See List of Ratifications at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=&DF=&CL=ENG (accessed July 2015).

encouraged to afford the widest possible mutual assistance to one another for the purpose of investigating cybercrime and collecting electronic evidence relating to criminal offences and to establish 24/7 cybercrime contact points to facilitate such cooperation.[70]

The CoE Convention was criticised by digital rights groups for mandating extensive national surveillance powers without addressing appropriate safeguards for the fundamental rights of individuals or including oversight mechanisms to ensure that these powers are not abused. Although the Convention has for the most part been superseded by corresponding provisions in the EU laws and policies discussed below, the CoE's standing Cybercrime Convention Treaty Committee (T-CY) has long called for a further additional Protocol to the Convention that would clarify and strengthen the rules on law enforcement access to data stored extraterritorially. This could undermine EU law and adds to concerns that the Convention is being used to establish a global framework for cybercrime surveillance by the 'backdoor'. This aspect is developed further in Section 4.

3.1.3. EU Cybercrime policy

The EU did not have a dedicated cybercrime policy until 2007. In 2001 the European Commission published a Communication on information security and combating computer-related crime.[71] Following on from the CoE Convention, this paved the way for EU Framework Decisions on attacks on information systems, fraud and non-cash means of payment, and the sexual exploitation of children (see further below in section 3.1.5).

Against this backdrop, the Commission's 2007 Communication 'Towards a general policy on the fight against cyber crime' prioritised the strengthening of operational law enforcement cooperation and EU-level training efforts; new measures to combat identity theft; a dialogue with industry and in particular ISPs with a view to initiating public-private agreements aimed at the EU-wide blocking of sites containing illegal content; devising a European model for the sharing of necessary and relevant information across the private and public sectors; the protection of critical IT infrastructure; and the collection of EU-wide statistics on cybercrime.[72]

Non-legislative measures and partnerships with industry were subsequently developed under the auspices of the EU Council. In 2008 the Council called for the establishment of national cybercrime 'alert platforms' and a European alert platform for reporting offences noted on the Internet; the establishment of joint investigation and inquiry teams in the Member States; a solution to the 'problems caused by … the anonymous character of prepaid telecommunication products'; mechanisms for blocking and/or closing down child pornography sites in Member States and a common EU 'blacklist' of such sites; and 'remote searches if provided for under national law, enabling investigation teams to have rapid

[70] See S. Carrera, G. González Fuster, E. Guild, and V. Mitsilegas (2015), *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental rights*, Centre for European Policy Studies, 22, 55, at http://www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers.pdf (accessed August 2015).

[71] European Commission (2001) Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by improving the Security of Information Infrastructures and Combating Computer-related Crime. Brussels, COM(2001) 890 final, 26 January.

[72] European Commission (2007), Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime, Brussels, COM(2007) 267 final, 22.5.2007.

access to information' – a provision the BBC reported as 'Police "encouraged" to hack more'.[73] In 2009, the Council mandated the establishment and funding of a European Financial Coalition (EFC) and national coalitions against child pornography on the Internet.[74] In 2010 it instructed the Commission to produce a feasibility Study for a European Centre against Cybercrime, located at Europol (as detailed below).[75] These demands were consolidated in the 2010 Stockholm Programme; the Internal Security Strategy (ISS) also listed cybercrime as one of five key action areas and called for new legislation to enhance network security with a system for reporting cybercrime and improved capabilities to deal with it.[76]

Since 2007 national law enforcement activities and EU actions in the area of cybercrime have been eligible for funding from the Programme Prevention of and Fight against Crime (ISEC), which is now part of the Internal Security Fund (ISF).[77] Initiatives funded under these programmes include an annual targeted call for proposals on 'Illegal Use of Internet', cybercrime 'Centres of Excellence', a European Cybercrime Training and Education Group (ECTEG), and various public-private dialogues and partnerships. A separate Safer Internet Programme, concerned with measures to protect children from harmful content and activities, has also been established.[78]

3.1.4. Institutional actors

A range of EU and external agencies and bodies support the development and implementation of EU cybercrime policy. **The centrepiece is EC3, the European Cybercrime Centre, which is part of Europol and has a broad law enforcement and police cooperation mandate**. ENISA has a cybercrime mandate that will be strengthened when the draft Directive on Network Information Security is adopted. Eurojust assists Europol and national cybercrime investigations and prosecutions; the European Police College (CEPOL) promotes cooperation and harmonisation of investigative methods for cybercrime among the law enforcement authorities of the Member States. CEPOL has developed a training course in conjunction with Europol on cybercrime forensics and digital evidence. The course is aimed at senior police officers and also covers cross-border cybercrime and 'best investigative practices' within the EU member states.[79]

[73] 2899th Council meeting - Justice and Home Affairs, Luxembourg, 24 October 2008, 14667/08 (Presse 299); and Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime, 2987th Justice and Home Affairs Council meeting, Brussels, 27-28 November 2008. See also 'Police "encouraged" to hack more', *BBC*, 5 January 2009, at http://news.bbc.co.uk/1/hi/technology/7812353.stm (accessed July 2015).

[74] Council Conclusions on the European Financial Coalition and national financial coalitions against child pornography on the Internet, 2969th Justice and Home Affairs Council meeting, Luxembourg, 23 October 2009.

[75] Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime, 3010th General Affairs Council meeting, Luxembourg, 26 April 2010.

[76] The Stockholm Programme – An open and secure Europe serving and protecting citizens (OJ C (2010) 115/1); and Internal Security Strategy for the European Union: Towards a European security model, approved by the European Council on 25 and 26 March 2010.

[77] Council Decision 2007/125/JHA of 12 February 2007 establishing for the period 2007-2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention of and Fight against Crime'.

[78] See European Commission website, Annual Work Programmes, Prevention of and Fight against Crime (I) at http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/prevention-of-and-fight-against-crime/index_en.htm (accessed July 2015); European Cybercrime Training and Education Group website, at http://www.ecteg.eu/ (accessed July 2015); and European Commission website, From a Safer Internet to a Better Internet for Kids, at http://ec.europa.eu/digital-agenda/en/safer-internet-better-internet-kids (accessed July 2015).

[79] Cybercrime forensics & digital evidence (16-20 November 2014), European Police College, at https://www.cepol.europa.eu/education-training/what-we-teach/residential-courses/20141115/112014-cybercrime-forensics-digital.

The EU has also set up a Computer Emergency Response Team (CERT-EU), whose role is to support European institutions in protecting themselves against intentional and malicious cyberattacks that could compromise their IT systems or otherwise threaten the interests of the EU. The European Defence Agency (EDA) and EU Military Staff are working on cyber-defence projects. All of these agencies are obliged or encouraged to cooperate with one another as the need arises, either through structured cooperation or ad hoc, informal channels. **Across these various bodies and organisations, the EU is building a community of technical and policy experts in the field of cybercrime. But whereas the main EU agencies work closely with the European Commission and have management boards where the Member States are represented, the European Parliament barely has a presence within this community**.

The EU also cooperates on a formal and informal basis with a host of intergovernmental bodies, including the G8 Lyon-Roma High-Tech Crime Group (which has its own network of national 24/7 cybercrime focal points); Interpol (structured cooperation with Europol); and ad hoc policy dialogues are held with the Council of Europe (Coe), the Organisation for Economic Co-operation and Development (OECD), the United Nations (UN), the Organisation for Security and Co-operation in Europe (OSCE), the North Atlantic Treaty Organization (NATO), the African Union (AU), the Association of Southeast Asian Nations (ASEAN) and the Organisation of American States (OAS). Bilateral cooperation is heavily focussed on the United States. This takes place under the auspices of the EU-US Working Group on Cyber-Security and Cyber-Crime, established in 2010.

3.1.5. Directive on attacks on information systems

Directive 2013/40/EU on Attacks against information systems was adopted in July 2013 and must be transposed by the Member States by September 2015.[80] It replaces and updates the 2005 Framework Decision of the same name, which was based on provisions in the CoE Cybercrime Convention and required Member States to criminalise 'hacking' offences, including unauthorised access to, or interference with, information systems and computer data.[81] Member States were also obliged to introduce common rules on criminal liability, criminal sanctions, jurisdiction, the exchange of information between law enforcement authorities, and the establishment of 24/7 contact points to assist in cross-border investigations.

The 2013 Directive builds on the provisions of the 2005 Framework Decision and extends its scope to 'botnet' attacks (the use of malicious software to take remote control of a potentially vast network of computers in order to stage large-scale, coordinated attacks – see Section 2), identity theft, the illegal interception of non-public transmissions of computer data from or within an information system, and the 'intentional production, sale, procurement for use, import, distribution or otherwise making available' of 'tools' used for committing cybercrimes. Ever since the CoE Cybercrime Convention was adopted, civil liberties groups have raised concerns that implementing its provisions could criminalise the tools used by security researchers (and so-called 'White Hat' hackers) for legitimate purposes.[82] Indeed in some states, prosecutorial discretion is the only thing that stands between this kind of cyber-security research and hacking charges.

[80] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[81] EU Council Framework Decision 2005/222/JHA on attacks against information systems.

[82] P. Sommer (2006), 'Criminalising hacking tools', *Digital Investigation*, 3(2), 68-72, at http://www.pmsommer.com/DI_hackingtools.pdf (accessed July 2015).

The Directive includes mandatory minimum terms of imprisonment of at least five years in cases where the hacking caused serious damage, was committed by a criminal organisation, and/or was perpetrated against the network of a critical infrastructure. It also encourages states to take 'aggravating circumstances' into account in developing sentencing frameworks for hacking offences. Under the Directive, the Member States are now required to respond to urgent information requests in no more than eight hours, and to collect statistical data and report on cybercrime incidents, investigations and prosecutions within their borders. The Directive also mandates single 24/7 points of contact for all requests for international cooperation.

3.1.6. Relationship between cybercrime and cybersecurity

There has always been a close link between EU cybercrime and cybersecurity policies: in 2001 the Commission issued parallel Communications on Cybercrime and on Network and Information Security; this twin-track approach was effectively consolidated in the 2013 Commission Communication on the Cybersecurity Strategy, which called for 'a more coordinated approach between Law Enforcement Agencies across the Union [in] cooperation with other actors'.[83] In particular, the Communication demands closer cooperation between ENISA, service providers and critical network infrastructure owners, the newly established European Cybercrime Centre, and EU bodies with a cyber-defence mandate.

3.1.6.1. ENISA

ENISA was established in 2004 to enhance the EU's capability to respond to network and information security problems.[84] Its mandate was expanded in 2013 to provide regular threat assessments; to more closely assist the EU and the Member States in achieving 'cyber-resilience' and implementing risk management strategies; to develop security standards for electronic products, systems and services; and to support the development of an internationally competitive network and security industry through the development of public-private partnerships.[85]

The headline breakthroughs in ENISA's 2014 Threat Assessment include taking down the 'GameOver Zeus' botnet and successful law enforcement cooperation against 'Silk Road 2' and other so-called 'darknet' sites. ENISA refers in its Threat Assessment to three headline threats: a 'massive stress' to core Internet security protocols (SSL and TLS); 'massive data breaches' highlighting the 'security vulnerabilities' of businesses and governments; and 'privacy violations, revealed through media reports on surveillance practices, [which] have weakened the trust of users in the Internet and e-services in general'.[86]

3.1.6.2. Critical Infrastructure Protection

There is significant overlap between the EU's critical infrastructure protection programme and EU measures to prevent cybercrime. Directive 2008/114/EC

[83] COM(2001) 890 final, 26.1.2001; and JOIN(2013) 1 final, 7.4.2013.

[84] Regulation 460/2004/EC of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

[85] Regulation 526/2013/EU of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

[86] ENISA (2014), Threat Landscape 2014: Overview of current and emerging cyber-threats, December 2014, at https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport (accessed July 2015).

designates European Critical Infrastructures (ECIs), obliging Member States, owners and operators to identify and implement proportionate measures to protect them. The main ECI sectors are energy (electricity, oil and gas) and transport (road, rail, air, internal waterways, ocean short-sea shipping and ports).[87] ENISA supports 'a holistic effort to ensure the security and resilience of ICT infrastructures, by focussing on prevention, preparedness and awareness, as well as to develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyber-attacks and cyber-crime [so] both the preventive and the reactive dimensions of the challenge are duly taken into account'.[88]

3.1.6.3 Draft NIS Directive

Proposed in February 2013 and still under negotiation, the draft EU Directive on Network and Information Security will impose obligations on critical electronic communications infrastructure operators to harmonise and strengthen cybersecurity across the EU.[89] Market operators include energy suppliers, banks, transport providers, the health sector, e-commerce platforms and application stores. At this stage Internet Security Providers (ISPs) appear to have lobbied successfully to be excluded from the scope of the Directive. EU Member States will be obliged to establish CERTs, nominate a competent authority (NCA) responsible for security breaches and major incidents, and devise and implement plans for dealing with them. NCAs will be required to share information with law enforcement agencies, form an EU network, and work with ENISA.

The most controversial aspect of the draft Directive concerns the provisions for the mandatory reporting of cybersecurity incidents. So-called 'breach reporting' will place obligations (with sanctions for failure to comply) on designated network operators to report cybercrimes and significant security incidents to NCAs, who must in turn share relevant information with their counterparts in other Member States and ENISA. The proposed Directive would be applied to 'public administrations' and 'market operators' in the banking sector, telecommunications companies, energy suppliers and e-commerce platforms, but some public bodies and Internet services (such as social networks) appear to have lobbied successfully to be excluded from its scope. Following a review of the E-privacy Directive, similar obligations already apply to the electronic communications sector and will apply to all data controllers under the draft General Data Protection Regulation, requiring companies to notify regulators and affected data subjects of data breaches.

Data protection and privacy can also be undermined by cybersecurity measures. ENISA has called upon the Article 29 working group on data protection to issue guidance on data protection applicable to CERTs and law enforcement agencies with a cybercrime mandate. **Digital rights advocates have gone further, calling for a strict separation of powers between law enforcement and security agencies responsible for preventing and investigating cybercrime and national security and intelligence agencies with offensive cyber-capabilities. Digital rights advocates argue that the new arrangements for breach reporting will strengthen the hand of national**

[87] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[88] European Commission (2011), Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security', Brussels, COM(2011) 163 final, 31 March 2011.

[89] 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 - Preparation for the informal trilogue, EU Council document 6905/15, 9 March 2015.

agencies tasked with cyber-espionage, and in so doing exacerbate the 'militarisation of cyberspace'.[90]

3.1.6.4 Cyber-defence

In its 2013 Communication on the Cybersecurity Strategy, the European Commission states that '[g]iven that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced'. It calls for these efforts to 'be supported by research and development, and closer cooperation between governments, private sector and academia in the EU'; for the EU to 'explore possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information infrastructures'; to 'improve cyber defence training and exercise opportunities for the military in the European and multinational context'; and to ''[p]romote dialogue and coordination between civilian and military actors in the EU [on] the exchange of good practices, information exchange and early warning, incident response, risk assessment, awareness raising and establishing cybersecurity as a priority'.[91]

3.2. Operational activities

3.2.1. Europol/EC3

Europol's mandate was extended to cybercrime in 2000, not long after the initial Europol Convention had entered into force.[92] Europol established a High-Tech Crime Centre (HTCC) in 2007, renaming it the Europol Cybercrime Centre in 2011 (EC3). But it was not until the EC3 was formally established in January 2013 that the agency took on a higher-profile role with increased resources dedicated to cybercrime.

EC3's mandate is to strengthen the law enforcement response to cybercrime in the EU and to help protect European citizens, businesses and governments.[93] **Because Europol already had a cybercrime mandate, the EU was able to establish EC3 without recourse to legislation or formal consultation of the European Parliament or other stakeholders**. The Council instructed the Commission to conduct a feasibility study, which was produced by RAND Europe, and a 2012 Commission Road Map paved the way for the establishment of EC3.[94] **The European Data Protection Supervisor (EDPS) stated that his informal comments and advice on the Commission's draft Road Map had been ignored.**[95]

EC3 is instructed to focus on cybercrimes committed by organised groups generating large criminal profits, such as online fraud; cybercrimes which cause serious harm to the victim,

[90] G. Burton, 'European Union security directive slammed by Ross Anderson', *Computing.co.uk*, 8 February 2013, at http://www.computing.co.uk/ctg/news/2242595/european-union-security-directive-slammed-by-ross-anderson (accessed July 2015).

[91] European Commission (2013), EU Cyber Security Strategy – open, safe and secure.

[92] Council Decision of 6 December 2001, extending Europol's mandate to deal with the serious forms of international crime listed in the Annex to the Europol Convention.

[93] See EC3 Website, at https://www.europol.europa.eu/ec3 (accessed July 2015).

[94] RAND Europe (2012), Feasibility Study for a European Cybercrime Centre Prepared for the European Commission, Directorate-General Home Affairs, Directorate Internal Security Unit A.2: Organised Crime, at http://ec.europa.eu/homeaffairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf (accessed July 2015).

[95] Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre, EU Council document 12406/12, 10 July 2012.

such as online child sexual exploitation; and cybercrimes (including cyber-attacks) targeting critical infrastructure and information systems in the EU.[96] To this end, **EC3 is designed to serve as a central hub for criminal information and intelligence related to cybercrime**, collecting data from the 'widest array of public, private and open source actors'; to support Member State operations and investigations, including by providing 'highly specialised technical and digital forensic support capabilities'. EC3 is also tasked with providing strategic analysis and establishing a comprehensive outreach function connecting cybercrime-related law enforcement authorities with the private sector, academia and other non-law enforcement partners.

EC3 also supports training and capacity building for Member State authorities and represents the EU law enforcement community in areas of common interest, such as research and development, Internet governance and policy development. Europol and ENISA signed a strategic cooperation agreement in 2014, and although it does not cover operational matters such as the exchange of personal data, there could be a role for EC3 to support the Member States in meeting the procedural obligations that will be imposed on different stakeholders by the NIS Directive.[97]

These different tasks are reflected in the organisation of the Centre. EC3 operational activities are organised around three analysis Focal Points: FP CYBORG, which focus on 'high-tech crime' such as the use of botnets, FP TERMINAL, which deals with payment fraud, and FP TWINS, which concentrates on child sexual abuse. The Cybercrime Intelligence Team (CIT), also located in the Operations part of EC3, implements the Centre's role as an 'intelligence hub'.[98] Since September 2014, **EC3 has formally hosted the Joint Cybercrime Action Taskforce (J-CAT), made up of cyber liaison officers from EU Member States** (Austria, France, Germany, Italy, Netherlands, Spain and the UK) **and non-EU law enforcement partners** (Australia, Canada, Colombia and the US). J-CAT is led by the Deputy Director of the UK's National Cyber Crime Unit.[99] Europol described J-CAT's task as 'pro-actively driving intelligence-led coordinated actions against key cybercrime threats and top targets' and credits it with the success of November 2014's Operation Onymous which resulted in 'more than 410 hidden services being taken down from the Darknet, the seizure of bitcoins worth approximately USD 1 million in cash, plus drugs, gold and silver'.[100] J-CAT is also credited with taking down the Ramnit botnet, which had infected 3.2 million computers around the world, in an operation involving Microsoft, Symantec, AnubisNetworks and CERT-EU, among other successes.[101] The establishment of

[96] European Commission (2012) Communication from the Commission to the Council and the European Parliament: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. Brussels, COM(2012) 140 final, 28 March 2012.

[97] ENISA, 'Fighting Cybercrime: Strategic Cooperation Agreement Signed between ENISA and Europol', press release, 6 June 2014, at https://www.enisa.europa.eu/media/press-releases/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol (accessed August 2015).

[98] Focal Points were established as part of the implementation by Europol of its 'new concept' for the Europol analysis work files (AWF), agreed upon by the heads of Europol national units in 2011. Analysis work files organise and make possible the analysis of data collected by Europol. Prior to the implementation of the new concept, there were as many as 23 AWF that operated as '23 different, largely disconnected databases'; see D. Drewer and E. Ellerman (2012), 'Europol's Data Protection Framework as an Asset in the Fight against Cybercrime', *ERA Forum*, 13(2), 381-395. The new concept merged the 23 AWF into only two, dealing with serious organised crime and terrorism. Within each of these AWF, Focal Points (and Target Groups) determine which data can be stored and by whom it can be accessed.

[99] National Crime Agency, 'Expert International Cybercrime Taskforce Is Launched to Tackle Online Crime', press release, undated, at http://www.nationalcrimeagency.gov.uk/news/news-listings/435-expert-international-cybercrime-taskforce-is-launched-to-tackle-online-crime (accessed July 2015).

[100] Europol, 'Mandate of Joint Cybercrime Action Taskforce Extended after Successful First Six Months', press release, 24 June 2015, at https://www.europol.europa.eu/latest_news/mandate-joint-cybercrime-action-taskforce-extended-after-successful-first-six-months (accessed July 2015).

[101] Europol, 'Botnet Taken Down through International Law Enforcement Cooperation', press release, 25 February 2015, at https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-

J-CAT not only reflects an effort to take into account the international dimension of cybercriminal activities, but also a change in the way cybercrime-related activities are approached at Europol. While Member State requests for support from Europol would normally come after an investigation has been opened at the national level and a need for European coordination identified, J-CAT reflects the assumption that cybercriminal activities are by definition cross-border and require coordination from the beginning.

3.2.2. National Cybercrime Units

As noted above, the G8, CoE and EU have all mandated the establishment of national Cybercrime focal points to deal with cross-border requests for police cooperation and mutual legal assistance. In some smaller Member States cybercrime remains part of the organised/serious crime agency remit, while the larger Member States have established dedicated cybercrime units. For example, in the UK, the National Cyber Crime Unit (NCU) has a mandate to address 'the most serious incidents of cyber crime' and pursue cybercriminals at the national and international level.[102] **But even recognising the need for a degree of operational secrecy, there is very little information or analysis as to the day-to-day activities of these units available to the public**. Given that these entities may also be tasked with developing and implementing investigative techniques – for example in the UK the NCU is tasked with assisting the National Crime Agency and wider law enforcement community with technical, strategic and intelligence support – this may represent a significant blind spot in terms of police accountability.

The concern here, as raised above in Section 2, is that **the 'cyber' prefix may be providing cover for new surveillance and investigative techniques that are only linked to cybercrime in the sense that the investigations concern the use of computers or internet traffic related to suspects in 'ordinary' investigations**. In the USA, the mass surveillance techniques employed by the National Security Agency (NSA) and Drug Enforcement Agency (DEA) have given rise to concerns about 'parallel construction'. 'Parallel construction' designates a process whereby evidence obtained through unwarranted surveillance is shared with other law enforcement bodies who then reconstruct the same evidence using a lawful method (for example a routine traffic stop), thus providing legitimate grounds for arrest or investigation and ensuring that the original surveillance cannot later be challenged in court.[103] In the EU, such practices would clearly breach the privacy and fair trial guarantees enshrined in the EU Charter of Fundamental Rights. Accountability and judicial control are therefore fundamental prerequisites for new law enforcement powers and investigative techniques to combat cybercrime or establish dedicated NCUs.

3.2.3. Relationship between cybercrime and other EU policy frameworks

3.2.3.1. Terrorism

EU law proscribes (or 'blacklists') terrorist organisations and criminalises many terrorist offences that can be committed online, including the provision of financial support to

cooperation (accessed July 2015); and Europol, 'International Operation Dismantles Criminal Group of Cyber-Fraudsters', press release, 10 June 2015, at https://www.europol.europa.eu/content/international-operation-dismantles-criminal-group-cyber-fraudsters-0 (accessed July 2015).

[102] National Cyber Crime Unit, UK National Crime Agency, at http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.

[103] 'DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations', *Electronic Frontier Foundation* (August 2013), at: https://www.eff.org/fr/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering (accessed October 2015).

blacklisted individuals or organisations, recruitment to terrorist groups, the dissemination of terrorist propaganda, and incitement to commit terrorist acts. Since 2005 the EU has been developing a strategy to combat radicalisation and recruitment to terrorist groups, but while the major goals of the strategy are in the public domain, **the details regarding its implementation have been largely withheld from scrutiny by the EP**.[104] The first EU "Radicalisation and Recruitment" Action Plan was adopted in 2005 but never published.[105] It was revised in 2008 to include 79 specific action points,[106] but the public was not allowed to know what these 79 measures were because all were redacted from the publicly available text. The Swedish Presidency, which oversaw the update of this plan, was "of the firm opinion that the revised version of the Radicalisation and Recruitment Action Plan should be a public document",[107] but its wishes were vetoed by other Member States. Most of the key subsequent documents relating to the EU's radicalisation and recruitment strategy have received the same treatment: of 90 documents on this topic listed on the Council's Public Register of Documents, many have been heavily redacted and over one third remain completely secret. Needless to say, **if parliaments and civil society are prevented from knowing what a particular EU strategy entails, it is impossible for them to even attempt to ascertain its legitimacy or effectiveness or otherwise play any part in the democratic process**.

In 2010 the EU adopted a standard form as part of what it called a 'standardised, multidimensional semi-structured instrument' for collecting data on people involved in radicalisation and recruitment to terrorism. It also instructed Europol to increase the EU's collective capabilities in this area.[108] With a March 2015 mandate from the EU Justice and Home Affairs Council, **Europol formally launched the EU Internet Referral Unit (EU IRU) to combat terrorist propaganda and related violent extremist activities on the Internet** on 1 July 2015, which built on its prior Check the Web initiative.[109]

EU IRU is described as a 'dedicated unit aimed at reducing the level and impact of terrorist and violent extremist propaganda on the Internet' [that] 'will identify and refer relevant online content towards concerned Internet service providers'. **No further details as to the criteria used by the IRU or subsequent procedures requesting the blocking or take-down of content believed to be unlawful have been published; nor has there been any parliamentary scrutiny of the mandate or powers of the new unit**.

In March 2014 the EU Council endorsed the principle that 'public-private partnership should be encouraged to tackle the challenge of radicalisation online'.[110] In January 2015, following the Charlie Hebdo attacks, the French government demanded that '[i]llicit content on the Internet must be identified more swiftly and taken down in a lasting manner where necessary'.[111] Three months earlier, in October 2014, the European Commission and EU

[104] Preventing Radicalisation and Recruitment to Terrorist Groups, EU Council document 10916/05, 15 May 2015.
[105] Ibid.
[106] Revised EU Radicalisation and Recruitment Action Plan, EU Council document 15244/08 EXT 1, 14 November 2008.
[107] Revised EU Radicalisation and Recruitment Action Plan, EU Council document 15374/09, 5 November 2009.
[108] Council conclusions on the use of a standardised, multidimensional semi-structured instrument for collecting data and information on the processes of radicalisation in the EU, 3010th General Affairs Council meeting, Luxembourg, 26 April 2010.
[109] Outcome of the Council Meeting, 3376th Council meeting - Justice and Home Affairs, Brussels, 12-13 March 2015; and Europol, 'Europol's Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda', press release, 1 July 2015, at https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda (accessed July 2015).
[110] Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism, EU Council document 9956/14, 19 May 2014.
[111] Combating terrorism and radicalisation: further strengthening the protection of the citizens of the European Union, EU Council document 5507/15, 23 January 2015.

Home Affairs ministers enjoyed an informal dinner with IT companies, including 'senior representatives of Google, Facebook, Twitter and Microsoft' to discuss 'the challenges posed by the terrorist propaganda on the Internet'.[112]

3.2.3.2. Organised crime

Framework Decision 2001/413/JHA harmonises and criminalises offences relating to fraud and combating fraud and counterfeiting of non-cash means of payment – primarily credit and debit cards.[113] Operational measures to target the perpetrators of such acts are set out in the Action Plan to implement the Concerted Strategy to combat cybercrime adopted in 2010.[114] Subsequent texts on 'cybercrime and the criminal misuse of the Internet' have not been published.[115]

The EU's operational model, which is centred around Europol, consists of opening an Analysis Work File on a particular topic (e.g. 'Cyborg', which focusses on cyber-attacks for financial gain); the setting-up of coordination mechanisms (Task Forces, joint investigation teams involving national cybercrime centres, etc.); the creation of crime reporting systems (such as the IRU, or Internet Crime Reporting Online System - ICROS, also known as the European Alert Platform); and the involvement of non-law enforcement actors where necessary through the Europol Outreach Programme.

Much of this cooperation takes place under the auspices of the newly-formed EU Standing Committee on Operational Cooperation (COSI) that adopts important non-legislative measures in these areas, with very few documents publicly available and no provision for scrutiny by the EP.[116]

2.2.3.3. Sexual exploitation of children

Framework Decision 2004/68/JHA on the sexual exploitation of children criminalises child prostitution, the coercion of children into sexual activities (including 'grooming'), and the production, distribution, supply and acquisition of child pornography.[117] Europol has long prioritised stopping the dissemination of child pornography on the Internet and has carried out a series of high-profile operations against websites and 'paedophile rings'.

The experience of cross-border cooperation in this field has also driven policy, with Member States sharing best practice with respect to blocking websites that host child pornography; the use of 'dedicated software for carrying out investigative activities on the Internet'; obtaining data from ISPs on the use of Internet portals, community portals, e-mail services, chat-rooms, online gaming, etc.; and requisite organisational structures and

[112] Joint statement Malmström - Alfano on the informal ministerial dinner with IT companies, European Commission statement, Luxembourg, 9 October 2014.

[113] Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment.

[114] Adoption of draft Council Conclusions on an Action Plan to implement the Concerted Strategy to combat cybercrime, EU Council document 8535/10, 16 April 2010.

[115] Implementation EU Policy cycle for organised and serious international crime: Draft strategic goals related to the EU crime priority 'Cybercrime and the criminal misuse of the internet', EU Council document 14452/2/11, 17 October 2011.

[116] A. Scherrer, J. Jeandesboz, and E.-P. Guittet (2010), *Developing an EU Internal Security Strategy, Fighting Terrorism and Organised Crime*, European Parliament Study, PE 462.423, Brussels.

[117] Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.

powers.[118] **These methods and practices have important implications that are not being discussed outside of the EU mechanisms for operational cooperation described earlier.** While successful EU action to combat cybercrime depends on close cooperation between law enforcement agencies and the private sector, by creating public-private partnerships for conducting surveillance on suspicious individuals or websites, for blocking or censoring content, or for investigating criminal activities, for example, **there is a significant risk that processes affecting fundamental rights enshrined in the EU Charter are hidden from public scrutiny, have a disproportionate impact (either generally or on already marginalised groups), cannot be challenged by affected parties, and undermine trust in governance on the part of internet users and digital rights advocates**.

The EU funds the European Financial Coalition (EFC) against commercial sexual exploitation of children online to bring stakeholders together and increase cooperation among them.[119] With the USA, the EU also supports the Global Alliance against Child Sexual Abuse Online.[120] The Commission describes these initiatives as 'a vehicle for further actions from the Member States supported by the Commission and the EC3'.[121]

3.2.4. Virtual currencies

Bitcoin was created in 2009 by an unknown person or entity using the name Satoshi Nakamato.[122] It uses encryption techniques to regulate the generation of currency units and verify the transfer of funds, operating independently of central banks. A public ledger distributed across the computers of the users of bitcoin containing the records of all of the bitcoin transactions that have ever been executed provides a 'trustless' proof mechanism, or 'blockchain' – one that dispenses with the need for the contractual relationships that substitute for trust in transaction counterparts or third-party intermediaries, like banks.[123] The algorithmic self-policing of the system is predicated on the elimination of the possibility to cheat or defraud, making it a particularly attractive model for economic trade. Bitcoin is the first and largest decentralised 'cryptocurrency', comprising around 90% of the total market capitalisation, but there are now hundreds of other 'alt coins' offering alternatives to bitcoin.[124] They employ different encryption protocols but are based on the same blockchain principles.

Although bitcoin is often described as an 'anonymous currency' – because it is possible to send and receive bitcoins without disclosing any personally identifying information – it is actually pseudonymous. If the addresses to which users send and receive bitcoins are revealed to belong to an individual, then their entire transaction history can be reconstructed from the blockchain. For many users of bitcoin, who access the currency through popular online wallet or exchange services, their participation entails linking their personal identity to their bitcoin holdings from the outset. Bitcoin for these users is effectively no more anonymous than a bank account (although this loss of anonymity takes place at the point of entry into the currency and is not a feature of the

[118] Combating sexual exploitation of children and child pornography in the Internet - strengthening the effectiveness of police activities in the EU Member States - Results of questionnaire, EU Council document 16069/11, 26 October 2011.
[119] See European Financial Coalition against commercial sexual exploitation of children online website, at http://www.europeanfinancialcoalition.eu/index.php (accessed July 2015).
[120] Declaration on the Launch of the Global Alliance against child sexual abuse online, European Commission Memo, Brussels, 5 December 2012.
[121] JOIN(2013) 1 final, 7.4.2013.
[122] See 'Bitcoin: A Peer-to-Peer Electronic Cash System', at https://bitcoin.org/bitcoin.pdf (accessed October 2015)
[123] M. Swan (2015) Blockchain: Blueprint for a new economy (O'Reilly).
[124] See Alternate cryptocurrencies - bitcoin alternatives, at http://altcoins.com/ (accessed October 2015)

bitcoin protocol itself).[125] Those seeking to preserve their anonymity have various options and services they can use – just as various techniques for de-anonymising transactions in the bitcoin ledger have been developed.

The EU does not yet have a formal policy toward virtual currencies (VCs). The European Banking Association (EBA) has proposed a regulatory framework and advised its members against using or holding VCs until such a framework is implemented.[126] For its part, the European Central Bank (ECB) has been monitoring the issue and produced several reports stressing that, although a lack of formal regulation poses various risks, the material risk to the ECB's tasks remains low.[127] VCs are currently the object of a regulatory debate in Europe and internationally, which takes into consideration not only risks but also the opportunities. This comes across very strongly in a recent report of the Canadian Standing Senate Committee on Banking, Trade and Commerce.[128] The report underlines the risks linked to cybercriminal activities and the banking system, but also and more prominently the promises of both the delivery system of de-centralised VCs for security and privacy as well as of virtual currencies themselves for economic growth. This was underscored recently by news that nine of the world's biggest banks have signed up to a project based on replicating the technical architecture of the bitcoin ledger to execute their own trades.[129]

Europol has taken a keen interest in VCs. In 2014 it held a joint meeting with the US Department of Homeland Security and law enforcement officials from 21 countries, where participants 'voiced concerns over the anonymity of financial transactions through some virtual currencies, such as Bitcoin, and the challenges this posed to 'following the money' during criminal investigations'.[130] In 2015 Europol produced a report, 'Exploring Tomorrow's Organised Crime', which it said reflected 'massive changes in the criminal landscape'.[131] The report warned of 'a virtual and global criminal underground made up of individual criminal entrepreneurs', arguing that VCs 'increasingly enable individuals to act as freelance criminal entrepreneurs operating on a crime-as-a-service business model without the need for a sophisticated criminal infrastructure to receive and launder money'.

[125] A Ludwin (2015) 'How Anonymous is Bitcoin? A Backgrounder for Policymakers', CoinDesk, at: http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/.

[126] EBA proposes potential regulatory regime for virtual currencies but also advises that financial institutions should not buy, hold or sell them whilst no such regime is in place. See EBA advisory, 4 July 2014, at https://www.eba.europa.eu/-/eba-proposes-potential-regulatory-regime-for-virtual-currencies-but-also-advises-that-financial-institutions-should-not-buy-hold-or-sell-them-whilst-n (accessed July 2015).

[127] ECB (2015), *Virtual currency schemes – a further analysis*, Frankfurt: European Central Bank, at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (accessed July 2015).

[128] Senate of Canada, Report of the Standing Senate Committee on Banking, Trade and Commerce (2015), *Digital Currency: You Can't Flip this Coin!*, June.

[129] 'Big banks consider using Bitcoin blockchain technology', BBC, 17 September 2015, at http://www.bbc.co.uk/news/technology-34278163.

[130] Europol, 'Cybercrime Experts Tackle the Criminal Exploitation of Virtual Currencies', press release, 17 June 2014, at https://www.europol.europa.eu/content/cybercrime-experts-tackle-criminal-exploitation-virtual-currencies (accessed July 2015).

[131] Europol, 'Massive Changes in the Criminal Landscape', press release, 17 June 2014, at https://www.europol.europa.eu/content/massive-changes-criminal-landscape (accessed July 2015).

Examples of cybercrime involving virtual currencies

Liberty Reserve was a centralised digital currency service based in San José, Costa Rica, that enabled its users to register and transfer money using only a name, e-mail address and date of birth. Deposits could be made using a credit card, bank wire, postal money order or money transfer service. These deposits were then converted into 'Liberty Reserve Dollars' or 'Liberty Reserve Euros', which were tied to the value of the US dollar and the euro respectively, or to ounces of gold. Once converted, deposits could be transferred to another account holder who could then withdraw the funds. No efforts were made by the site to verify identities of its users, in breach of the due diligence requirements established by international anti-money laundering regimes, and Costa Rican regulators refused to issue a business license. After a multi-year investigation by officials in 17 countries, the Liberty Reserve website was taken offline on 24 May 2013 amid allegations that it had handled $6 billion of criminal proceeds. One of Liberty Reserves co-founders, Vladimir Kats, was arrested in New York and ultimately pleaded guilty to money laundering and operating an unlicensed money transmitting business. Other senior staff also entered into plea bargains but co-founder Arthur Budovsky, who was arrested in Spain and extradited to the USA, has pleaded not guilty and is still awaiting trial. He claims that Liberty Reserve was conceived simply as 'PayPal for the unbanked' (i.e. people without a bank account). At the time of its closure, Liberty Reserve had more than 1 million registered users, 200,000 of which were from the United States. The closure of the site also led to many individuals using the service for legitimate reasons losing access to their money.[132]

Mt. Gox, based in Tokyo, Japan, was the world's largest bitcoin exchange. It filed for bankruptcy protection in February 2014 when it came to light that 850,000 bitcoins, then worth $450 million, had disappeared or been stolen by hackers. Mt. Gox said it also lost $27 million in cash. Some 650,000 bitcoins still remain unaccounted for. Mark Karpeles, the French CEO of Mt. Gox, is facing criminal charges for fraud and embezzlement in Japan relating to his use of company funds, but he has not been charged with offences covering the vast total of missing bitcoins. According to independent security researchers Wiz Sec, the bitcoins appear to have been stolen using a robot programme operating in the Mt. Gox exchange nicknamed 'Willy Bot', which was buying hundreds of thousands of bitcoins with fake money by creating new accounts and setting their balance to millions of dollars.[133] Speculation is rife as to the location and identity of the hackers behind 'Willy Bot'.

CTB (Curve-Tor-Bitcoin) Locker is malicious software (or 'malware') used by criminals to encrypt data on an individual's computer and then demand a ransom from the victim in order to receive the decryption key. CTB Locker builds on earlier versions of 'ransomware' such as 'Gameover' and 'CryptoLocker'. Once a computer user has been tricked into installing the malware on their computer (e.g. by opening an attachment delivered by email), the ransomware encrypts data on their hard drive and provides the user with instructions on how to pay for the decryption key with bitcoins. The ransomware is linked to a server via the Tor (The Onion Router) network, which provides anonymity to its users.[134] The infrastructure is relatively easy to use, providing an 'open-source' means for new criminals to enter the ransomware business. Industry reporting suggests that up to 35% of CTB Locker victims reside within Europe.

[132] 'Liberty Reserve: Serving the unbanked or the underworld?', pymnts.com, 21 April 2005, at: http://www.pymnts.com/in-depth/2015/liberty-reserve-serving-the-unbanked-or-the-underworld/ (accessed October 2015)

[133] 'After the CEO's Indictment the Great Mt. Gox Bitcoin Mystery Deepens', The Daily Beast, 14 September 2015, at: http://www.thedailybeast.com/articles/2015/09/14/after-the-ceo-s-indictment-the-great-mt-gox-bitcoin-mystery-deepens.html (accessed October 2015)

[134] 'All You Need to Know About CTB Locker, the Latest Ransomware Generation', Heimdal Security, 28 January 2015, at: https://heimdalsecurity.com/blog/ctb-locker-ransomware/ (accessed October 2015)

Law enforcement discourse about the legitimacy and impact of virtual currencies mirrors wider debates about how to address the increased take-up of encryption technologies highlighted in the previous Section. In 2014 a joint conference by CEPOL, the EU Police Training College, and the Latvian EU Presidency stressed '[t]he need to consider the practical challenges that "encryption by default" would present to law enforcement authorities and look into the technological solutions that might facilitate or overcome these challenges, taking into account the privacy and human rights implications'.[135] In the UK the government has threatened to ban newly encrypted communications applications like WhatsApp; in the US law enforcement agencies have been demanding encryption keys from the likes of Apple and Microsoft.

While these debates highlight the tremendous effect that the discourse on cybercrime can have on fundamental rights, including the right to privacy in communications and online transactions, **simplistic attempts to frame encrypted services as merely helping criminals and terrorists miss the point that the legitimate uses far outweigh the illegitimate ones**. The growing use and popularity of encrypted communications is first and foremost an economic response to the lax approach to information security and the kind of unchecked government surveillance policies revealed by Edward Snowden. Similarly, blockchain technologies and bitcoins are disrupting established currencies and transaction systems because they are based on sound design that **offers numerous economic advantages over incumbent business models**.

This is not to play down the significance of the use of these technologies by criminals in enterprises such as 'Silk Road' (as further developed in Section 2 above): law enforcement agencies certainly need to develop the skills to investigate and prosecute novel criminal enterprises (like Interpol, setting up its own virtual currency to train police forces). Rather, it is to suggest that **simply bemoaning their emergence and floating unworkable ideas like banning or undermining encryption will be neither helpful nor fruitful**.

Demands for blanket surveillance powers threaten to undermine information security protocols and derail the emergence of exciting disruptive technologies, but as the examples developed in the above box show, the challenge is as much about keeping the users of new technologies safe which, paradoxically, requires that information and communication security protocols are strengthened. This is not an area where some notional 'balance' between security and fundamental rights can be achieved; it is either better security or back-door surveillance that creates vulnerability for all users.

3.2.5. Oversight and accountability

The minimal scrutiny of the EU's operational activities in the area of cybercrime mean that key EU policy decisions – regarding, for example, the level of surveillance of Internet users, the procedures for blocking or censoring content on the Internet, law enforcement requirements vis-à-vis network operators, and the use of 'hacking' and Internet surveillance tools by law enforcement agencies – are effectively being left in the hands of law enforcement and cybersecurity agencies.

Cross-border investigations and joint operations have minimal political or judicial oversight at the EU level. **Although the EP has enjoyed co-decision over important legislative acts, it risks being marginalised altogether with respect to the implementation**

[135] Outcome of the CEPOL - Presidency conference on cybercrime: Strategic Approach on Cybercrime. Future Challenges in Tackling Online Criminality, 25-27 March 2015, Jūrmala, Latvia, EU Council doc. 7368/15, 8 April 2015.

and review of those policies by the exercise of delegated powers, EU agency discretion and non-legislative decision-making bodies such as COSI.

The institutional architecture of EU cybercrime policy presented in this section raises significant challenges in terms of policy-making and accountability. These political challenges are enhanced by the challenge of cooperation and fundamental rights, as the next section shows.

4. CYBERCRIME: THE CHALLENGE OF JURISDICTON, COOPERATION AND FUNDAMENTAL RIGHTS SAFEGUARDS

KEY FINDINGS

- Cybercrime is said to complicate the traditional territorial foundations of law and operational cooperation. If there is room for improvement in existing cooperation frameworks, claims of their inefficiency are not corroborated by objective evidence
- If there are challenges at play from the law enforcement perspective in terms of the speed of access under MLA agreements, remedying these challenges must be accomplished with a commitment to the rule of law and the proper safeguarding of privacy and the rights of defence for suspected persons.
- There are increasing calls for law enforcement to have access to data outside MLA agreements. Yet state authorities operating with unmediated access outside existing legal channels would pose serious challenges to the rule of law and jeopardise due process and the successful prosecution of cybercriminal offences.
- While third-country access to data outside of MLA agreements is problematic in terms of fundamental rights, it is of particular concern regarding the US, because of the differences in EU and US approaches to data protection and the lack of effective judicial privacy safeguards afforded to EU citizens on US territory.

With regard to cybercrime, law enforcement can face overlapping and conflicting legal frameworks and guidelines for practice, particularly when the international and cross-border nature of cyber activity is taken into account. This raises important questions in terms of fundamental rights. This section argues that operational challenges in cybercrime law enforcement do not change the obligation of EU institutions and Member States to ensure the safeguarding of EU fundamental rights in any operating framework of internal or transnational cooperation in law enforcement and criminal justice. It details these operational challenges with a focus on jurisdiction, information sharing, the role of the private sector, and the implications of US ownership of significant Internet infrastructure (4.1). Within this context, it then focusses on the implications for the right to privacy and data protection (4.2).

4.1. Operational challenges: jurisdiction, information sharing and cooperation

4.1.1. The jurisdictional challenge

At the 2015 Academy of European Law seminar on Countering the Illegal Use of the Internet, one of the challenges most frequently referred to by members of the European legal community was the `complexity of cybercrime cases from a jurisdictional perspective'.[136] Similarly, the 2014 EC3 Internet Organised Crime Threat Assessment (iOCTA) report plainly stated that 'the whole concept of a territorially based investigative approach conflicts with the borderless nature of cybercrime.'[137] The report on EC3's first year in operation furthermore stated that while 'investigations in the past had a predominantly national focus with some international links, the emphasis has now shifted towards the coordination of international cybercrime operations.'[138] This points to the changes in the approach adopted within Europol towards cybercrime operations with the establishment of J-CAT, as discussed previously in Section 3.

The media regularly refer to European cybercrime operations resulting in multiple arrests and cybercrime network takedowns.[139] Yet Europol officials underline the lack of cybercrime cooperation from particular parts of the world. Former EC3 Director Troels Oerting, for instance, expressed frustration at Russia's lack of cooperation with J-CAT.[140] The 2014 iOCTA report expressed the need for more Russian language capacities in EU law enforcement.[141] Furthermore, the growing use of the Internet in certain parts of the world is often mentioned in cybercrime threat assessments: 'Especially in Southeast Asia, South America and Africa the number of [Internet] users are (sic) expected to grow fast. Since these are regions with which limited judicial cooperation exists, the EU law enforcement response against perpetrators from those territories will face an increased level of complexity and constraints.'[142]

Across the spectrum of cybercrime prevention, investigation, and prosecution, **the particular geography of the digital environment is said to complicate the traditional territorial foundations of law.** Law enforcement bodies make continuous reference to how traditional legal structures stand in the way of operations. However, as described in section 4.2 hereafter, an updated legal framework designed to overcome these challenges must foreground fundamental rights concerns. This is essential to ensure due process and the successful prosecution of cybercriminal offences.

4.1.2. Information sharing

In addition to the cross-border aspects of cybercrime, one of the most commonly mentioned challenges by cybercrime law enforcement officials is the ability to quickly obtain data and information across traditional, territorial jurisdictional boundaries.

Cybercrime law enforcement actors assert the need to speed up exchanges and ease barriers to information sharing. In a 2015 interview, Troels Oerting stated that '[o]ur mutual legal assistance process is not sufficient anymore. There is a big need for speeding

[136] ERA Seminar on Countering the Illegal Use of the Internet, 2015.

[137] European Cybercrime Centre (2014), 'The Internet Organised Crime Threat Assessment: Executive Summary and Recommendations', 9, at http://tinyurl.com/obbgf4g (accessed June 2015).

[138] European Cybercrime Centre (2014), 'First Year Report', 4, at http://tinyurl.com/pjdtubv (accessed June 2015).

[139] For instance, the November 2014 EC3-coordinated operation, which saw the arrest of over 100 persons who used stolen credit cards to pay for flights, required the participation of 49 law enforcement agencies, multiple banks, 64 airlines, the International Air Transport Association, Interpol, and Ameripol. See 'Europol Arrests 118 People Using Stolen Credit Cards to Pay for Flights', *The Guardian*, 28 November 2014, at http://tinyurl.com/obw745b (accessed June 2015). See also 'Europol Shuts Down Ramnit Botnet that Infected 3.2m Computers', *The Guardian*, 25 February 2015, at http://tinyurl.com/ol9mwnj (accessed June 2015), which describes another EC3 operation conducted in February 2015, which shut down seven servers used by the Ramnit botnet. Britain, Germany, Italy, the Netherlands participated in this operation, with the assistance of AnubisNetworks, Microsoft and Symantec.

[140] 'Europol Launches Taskforce to Fight World's Top Cybercriminals', *The Guardian*, 1 September 2014, at http://www.theguardian.com/technology/2014/sep/01/europol-taskforce-cybercrime-hacking-malware.

[141] European Cybercrime Centre, 'The Internet Organised Crime Threat Assessment', 14.

up the judicial cooperation. One thing is that police cooperation needs speeding up, but also the judicial because [evidence cannot be obtained].'[143] Oerting is not alone in voicing criticism of mutual assistance efforts, such as the EU Convention on Mutual Assistance in Criminal Matters. The 2014 Europol iOCTA report describes the need for 'more efficient and effective legal tools, taking into account the current limitations of the Mutual Legal Assistance Treaty (MLAT) process, and further harmonisation of legislation across the EU where appropriate'.[144] The issue was also raised at a 2015 ERA seminar, where it was stated that mutual assistance procedures are 'too cumbersome' for cybercrime law enforcement, whereas international cooperation through Europol and Eurojust was said to expedite cybercrime investigations.[145] These claims raise specific legal challenges, as described further in Section 4.2.

4.1.3. The role of the private sector in cybercrime law enforcement

The issue of cybercrime law enforcement cooperation and information sharing is complicated by the reality of private sector ownership of digital infrastructure. In terms of information sharing, commentators have noted **the private sector's increased reluctance to share data following the Snowden revelations**.[146] An industry representative stressed the importance of 'drawing a distinction between intelligence-gathering for national security purposes (tainted by the Snowden revelations) and approved criminal inquiries'.[147] According to EC3, the private sector's caution in sharing data is not new: 'Challenges to the effective initiation and coordination of cybercrime operations have been EC3's inability to receive essential evidence and intelligence directly from private industry. Under-reporting of cybercrime to law enforcement, for fear of brand damage, has resulted in police not having the fullest picture of the extent and trends'.[148]

Corporations, which are subject to the national laws of the countries in which they are based, are not bound by international human rights laws, which apply only to states and governments. Jurisdictional tensions surround the issue of national laws and Internet companies operating internationally. Several cases have spotlighted the public-private information sharing landscape, such as the case in the Belgian courts of Yahoo!. The case concerned whether or not the company was obliged to provide data about its e-mail users to law enforcement. The case largely hinged upon jurisdictional questions over whether US-based Yahoo! was compelled to provide data directly to law enforcement agencies based on the Belgian Criminal Procedure Code. In reference to the relationship of the private sector to international human rights law, **the UN recently launched the Guiding Principles Reporting Framework focussed on how companies respect human rights in business practice. However,** as Korff emphasises, **the framework addresses how states might act against violations by companies but does not deal with situations 'where states make demands of companies that would lead companies into violations of international human rights law'**.[149] This limits the framework's significance in the field of cybercrime law enforcement, where the key concern is state law enforcement agencies making data requests to private companies. Other recent efforts

[142] European Cybercrime Centre, 'First Year Report', 26.
[143] 'Trouble with Russia, Trouble with the Law: Inside Europe's Digital Crime Unit', *The Guardian*, 15 April 2015, at http://tinyurl.com/jwk7gl9 (accessed July 2015).
[144] Europol, *The Internet Organised Crime Threat Assessment (iOCTA)*, 13.
[145] ERA Seminar on Countering the Illegal Use of the Internet (2015).
[146] 'Has the NSA's Mass Spying Made Life Easier for Digital Criminals?', *The Guardian*, 7 March 2014, at http://tinyurl.com/m8482uz (accessed July 2015).
[147] ERA Seminar on Countering the Illegal Use of the Internet (2015).
[148] European Cybercrime Centre, 'First Year Report', 15.
[149] D. Korff (2014), 'Rule of Law on the Internet and in the Wider Digital World', Council of Europe Commissioner for Human Rights Issue Paper, 12.

include a Council of Europe study on the Internet Corporation for Assigned Names and Numbers (ICANN)'s potential role in defending human rights and fundamental freedoms online.[150]

Beyond the question of information sharing, concerns have emerged recently about possible deliberate backdoors designed into digital security products by the private sector at the behest of state intelligence agencies (the security firm RSA was said to have adopted two encryption tools developed by the NSA in order to increase the agency's ability to intercept digital communications).[151]

4.1.4. US ownership of digital infrastructures and impact of US law on international cybercrime enforcement

This issue of the private sector's role in cybercrime law enforcement is closely related to another challenge: the fact that the US and US-based corporations play leading roles in the functioning of the Internet. **Thus US legal frameworks have a significant impact on cybercrime law enforcement and the handling of personal data around the world**. As discussed above, a private company is subject to the national law of the countries in which it operates. This is of particular concern because US human rights frameworks differ from international standards of human rights law. Whereas international human rights law since 1945 has been aimed at all human beings regardless of nationality, US rights guarantees related to freedom of speech and association as well as protection from 'unreasonable searches' apply only to US citizens. **This has implications for European and international law enforcement, especially after the revelations of mass surveillance by the NSA**. A 2013 European Commission Communication spoke of damaged trust in what had been close EU-US cooperation: '[R]ecent revelations about US intelligence collection programmes have negatively affected the trust on which this cooperation is based. In particular, it has affected trust in the way personal data is processed'.[152]

4.2. Upholding fundamental rights and EU rule of law in cybercrime law enforcement

If law enforcement agencies argue that traditional, territorial legal structures stand in the way of their operations because of the 'borderless nature of cybercrime,' it is imperative to consider what this means for the rights to privacy, data protection, freedom of expression, and the rights of suspected persons.[153] Similarly, just as law enforcement bodies state that the speed of technological change is an operational challenge and express a desire for faster data exchange, it is also important to consider the implications of rapid technological change in the protection of fundamental rights. For example, as the Electronic Frontier Foundation (EFF) noted in 2011, the CoE Convention on Cybercrime was developed a decade earlier when traffic data was considered 'less sensitive' and more readily available to law enforcement.[154] Currently traffic data, as logged by mobile phone companies and

[150] M. Zalnieriute and T. Schneider (2014), *ICANN's Procedures and Policies in the Light of Human Rights, Fundamental Freedoms and Democratic Values*, Council of Europe Report, DGI(2014)12, at http://tinyurl.com/o35gzq5 (accessed June 2015).

[151] 'NSA Infiltrated RSA Security More Deeply than Thought', *Reuters*, 31 March 2014, at http://tinyurl.com/ldeq7fs (accessed June 2015).

[152] European Commission (2013), Rebuilding Trust in EU-US Data Flows, COM/2013/0846 final, 5, at http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf (accessed July 2015).

[153] *The Internet Organised Crime Threat Assessment (iOCTA)*, 9.

[154] K. Rodriguez (2011), 'Dangerous Cybercrime Treaty Pushes Surveillance and Secrecy Worldwide', *Electronic Frontier Foundation*, 25 August, at http://tinyurl.com/3p6r84q (accessed July 2015).

ISPs, is very sensitive because it is linked to an individual's online identity, personal information and contacts. Legal instruments for cyber law enforcement, and what they imply for the protection of fundamental rights, can lag behind changes in technology. A report published by the CoE's Commissioner for Human Rights identifies three limitations of the CoE Convention: it limits the human rights clause to procedural law; there are conflicting applications of the Convention in different national legal systems; and there is a 'contentious provision on cross-border 'pulling' of data by law-enforcement agencies'.[155] Civil liberties groups are equally critical in their assessment of the Convention's implications for law enforcement and fundamental rights. The EFF called it '[t]he '[w]orld's '[w]orst Internet [l]aw'.[156] It has cited concerns about the Convention's 'failure to specify proper level of privacy protection necessary to limit the over-broad surveillance powers it grants law enforcement agencies', particularly in light of the broadly different applications and different national constitutional standards of rights protection.[157]

The 1995 Data Protection Directive (Directive 95/46/EC) has long been the cornerstone of EU data protection guidelines. More specific rules concerning police and judicial cooperation are provided in complementary instruments such as the 2008 Framework Decision (2008/977/JHA). Declaration 21 of the Lisbon Treaty acknowledges 'that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 B of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields'.[158] The existing framework is generally fragmented across EU policy areas. In its Action Plan on implementing the Stockholm Programme, the Commission expressed the need for the fundamental right to personal data protection to be evenly applied across all EU policy areas, including law enforcement and crime prevention.[159] In 2010 it issued a Communication on a comprehensive EU approach to personal data protection.[160] Following on from this call, **there are changes afoot in the EU legal landscape concerning data, rights and law enforcement**. There are proposals now for a new European General Data Protection Regulation (GDPR) to replace the Data Protection Directive.[161] In parallel with the proposal for a GDPR, the Commission adopted a policy communication setting out the Commission's objectives (5852/12).[162] It also adopted a Directive on data processing for law enforcement purposes (5833/12), which is intended to replace the 2008 Data Protection Framework Decision.[163]

[155] Korff, 'Rule of Law on the Internet and in the Wider Digital World', 93.

[156] D. O'Brien (2006), 'The World's Worst Internet Law Sneaking Through the Senate', *Electronic Frontier Foundation*, 3 August, at http://tinyurl.com/p86ed7o (accessed 24 June 2015).

[157] Rodriguez, 'Dangerous Cybercrime Treaty'.

[158] Declaration 21 annexed in the Final Act of the Intergovernmental Conference adopting the Treaty of Lisbon, 13/12/2007.

[159] COM(2010)171final.

[160] European Commission, Communication on A comprehensive approach on personal data protection in the European Union, COM(2010)609 final, 4 November 2010.

[161] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.

[162] European Commission, Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final, Brussels, 25 January 2012.

[163] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25 January 2012, Brussels.

4.2.1. Rights protections in the existing field of cooperation

As mentioned previously, practitioners frequently cite shortcomings in the MLA instruments concerning information exchange in cybercrime law enforcement, especially when it comes to the time required to obtain evidence across borders. A recent study finds that claims of inefficiency in existing cooperation frameworks are however not corroborated by objective evidence.[164] Assessment surveys conducted for a workshop organised by Eurojust and a report by the CoE Convention Committee regarding the efficiency of MLA agreements report excellent cooperation; the reports also reveal that obstacles in particular cases 'are usually overcome through bilateral case consultations and daily contacts between central authorities'.[165] **Thus, while the claim of MLA agreement inefficiency lacks empirical evidence, the frequency of the claim warrants attention**, not least because circumventing existing internal and external judicial and law enforcement cooperation commitments would pose significant challenges to the rule of law and fundamental rights.

Existing EU data protection and privacy law establishes normative standards and clear limits to direct access to private databases by state authorities. Article 8 of The Charter of Fundamental Rights of the EU enshrines personal data protection as a fundamental right, while Article 8 of the European Convention on Human Rights protects the human right to privacy. The principle of the individual's right to personal data protection is also established in Article 16(1) of the TFEU, while Article 16(2) introduces the legal basis for rules concerning data protection, also in police and judicial cooperation. **EU institutions and Member States are obliged to safeguard these EU fundamental rights in operating frameworks governing internal or transnational cooperation in law enforcement and criminal justice**.

The Court of Justice of the European Union (CJEU) ruling on the Digital Rights Ireland case is critical here in terms of its impact on limiting the collection and exchange of personal data and for the emphasis it places on the principle of proportionality.[166] The ruling not only struck down the Data Retention Directive, but its broader relevance to data retention measures includes the finding that retention measures that are not proportionate and targeted are in violation of EU law, ineffective, and incompatible with data protection principles.[167] **The Court's reasoning and findings are relevant for assessing the legality and proportionality of cybercrime law enforcement cooperation pertaining to data exchange and processing**.

It should be noted that the right to data protection also covers data security. This is protected in the EU Charter and Article 8 of the European Convention on Human Rights. It is also explicitly referred to in the Data Protection Convention of the CoE, the current 2008 Data Protection Framework Decision and in the proposed GDPR (analysed in section 4.2.3). **This means that decisions dealing with access to encryption methods, which could endanger the security of data in allowing for (future) access to law enforcement authorities or obliging private actors to organise their data systems accordingly, would contradict the commitment to data security as a component of the right to data protection.** Data security is also at stake with regard to the issue of national

[164] Carrera, González Fuster, Guild, and Mitsilegas, *Access to Electronic Data*, 65-72.

[165] Ibid., 69

[166] Judgment of the Court of Justice of the European Union in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014.

[167] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L.105

governments or public authorities having a key or master key to encryption, as previously underlined in section 2.2.

The CoE Cybercrime Convention's obligations on Member States must also be consistent with EU law and fundamental rights. Two articles of the Convention are of particular concern in terms of developing a fully adequate framework of rights protection. Article 26 allows States to distribute information from an ongoing investigation to other States if the information is thought to be helpful to the other party. These disclosures do not have to be recorded, and the Article only stipulates that they must be 'within the limits' of the law of the sharing country. More troubling, Article 32 of the CoE Convention, concerning 'trans-border access to stored computer data with consent or where publicly available,' leaves considerable room for manoeuvre in terms of cross-border disclosure and consent. In his analysis of Article 32 as it is currently applied, Korff concludes that the situation is one 'where **cross-border access to personal data by national law-enforcement agencies is becoming effectively unregulated and close to arbitrary**'.[168]

Furthermore, discussions on a revised Convention have raised the possibility of unmediated transnational access to data outside of MLA agreements. The Cybercrime Convention Committee has put forward controversial proposals aimed at amending Article 32 in this respect.[169] Similar discussions have taken place within Cybercrime@Octopus, a CoE project regarding a new instrument for cross-border personal data access by States.[170] **It is thus of crucial importance that the details of any such protocols be drafted in consultation with parliaments and civil society groups and that the rule of law and respect for EU fundamental rights be ensured**.

The EU is committed to MLA agreements, which form the basis for legal evaluations of cross-border evidence requests in ongoing criminal investigations through legally mediated channels. Thus MLA agreements are crucially important in upholding fundamental rights in cybercrime law enforcement. They are the most important instruments for making lawful decisions regarding assistance in evidence gathering from foreign jurisdictions – even if more informal procedures are sometimes preferred. The EU-US MLA is particularly important given requests coming from the US for access to data held by companies under EU jurisdiction. **While third-country access to data outside of MLA agreements is problematic in terms of fundamental rights, it is of particular concern regarding the US, not least because of the differences in EU and US approaches to data protection and the lack of effective judicial privacy safeguards afforded to EU citizens on US territory**. In that regard, the EU-US data protection 'Umbrella agreement' negotiations have just been finalised at the time of writing. In the Commission's words, this agreement 'will provide safeguards and guarantees of lawfulness for data transfers, thereby strengthening fundamental rights, facilitating EU-US law enforcement cooperation and restoring trust'.[171] **The Commission's proposal will require the Council's authorisation, as well as the consent of the EP. This will provide an opportunity for the EP to review the provisions of the agreement**.

[168] Korff, 'Rule of Law on the Internet and in the Wider Digital World', 104.

[169] See Cybercrime Convention Committee (2014) 'T-CY Guidance Note #3: Transborder Access to Data (Article 32), [T-CY (2013)7 E] Council of Europe, Strasbourg, at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a (accessed August 2015).

[170] For a description of this discussion, see Korff, 'Rule of Law on the Internet and in the Wider Digital World', 105.

[171] European Commission - Fact Sheet, Questions and Answers on the EU-US data protection 'Umbrella agreement', Brussels, 8 September 2015

In addition to MLA agreements, the European Investigation Order (EIO) will become the principal instrument ordering evidence exchange and mutual legal assistance between Member States. The **EIO provides clear limits to judicial cooperation on both human rights and proportionality grounds, and the human rights safeguards enshrined in this instrument also constitute benchmarks for the external action of the EU and Member States in the field**.

There are increasing calls for law enforcement to have access to data outside MLA agreements, particularly in reference to data held by private companies. Yet **state authorities operating with unmediated access outside existing legal channels would pose serious challenges to the rule of law. This could fuel mistrust in transatlantic relations and among the general public, particularly considering the Snowden revelations,** which drew attention to the incompatibility of mass personal data surveillance with European rule of law.[172]

Given the frequency with which law enforcement authorities point to the inadequacies of current legal instruments, it is important to consider different scenarios and policy recommendations for future action. A recent Centre for European Policy Studies (CEPS) report, focussing on the transatlantic context and third-country access to data held by private companies for the purposes of law enforcement, maintains that **existing legal models should be adhered to and can be made more effective 'through a combined approach focussed on bilateral case consultations, day-to-day contacts, stronger political commitments, more effective use of existing tools and sound financial, technological and human resources investments in their implementation'**.[173] The report considers three possible policy paths that could help ensure the rule of law, foster trust-based approaches and ensure fundamental rights in the broader field of cybercrime law enforcement. These recommendations were drafted with specific reference to EU-US mutual legal assistance agreements, but they hold broader applicability and relevance for cybercrime law enforcement policy paths.

The first envisaged path avoids legislative reform and focuses on enhancing the existing MLA model **with better data collection, tracking and transparency of data requests made under the MLA model**. Proposed measures include the establishment of an independent and objective evaluation system that gathers statistical information on the frequency, quantitative use and scope of MLA requests. The goal of this information gathering is two-fold: to develop a guide for practitioners to overcome obstacles and streamline procedures and to develop a universal tracking system to enhance transparency with a more active role for Eurojust under close supervision of the EP and data protection authorities. This first option also stresses **the avoidance of unmediated access to electronic data amongst EU Member States and regional bodies** and the avoidance of amending existing EU legal instruments and standards on criminal justice cooperation in favour of strengthening bilateral commitments, daily contacts, and political commitments to existing legal channels.

The second path envisages legislative reform in light of the post-Lisbon Treaty context, which has reformed EU legal competence related to criminal justice and police cooperation.

[172] See: LIBE Committee, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 2014. For an in-depth analysis, see D. Bigo, S. Carrera, N. Hernanz, J. Jeandesboz, J. Parkin, F. Ragazzi, and A. Scherrer (2013), *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU Law*, Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), PE 493.032, Brussels.

[173] Carrera, González Fuster, Guild, and Mitsilegas, *Access to Electronic Data*, ii.

In particular, as mentioned earlier, **the benchmarks and safeguards enshrined in the EIO could form the minimum basis for revising existing MLA frameworks**. If there were to be revisions, the EIO and EU Charter of Fundamental Rights benchmarks would have to function as the minimum standards for new provisions and the European Commission and the EP should ensure proper codification to guarantee consistent implementation and avoid further fragmentation of EU criminal law across the Justice Area. It is stressed that legislative reform should avoid replicating the 'mediator' role given to Europol in the Terrorist Finance Tracking Program (TFTP), which has been challenged on the basis of a lack of proper judicial oversight and independent scrutiny and transparency of decisions.

The third option relates to EU external criminal justice cooperation and envisages a Transatlantic Investigation Order, developed under close judicial scrutiny, which would use existing EIO benchmarks as the basis for cooperation. The goal would be to export and extend the EU principle of mutual recognition in criminal justice cooperation. While this particular proposal refers specifically to the EU-US context, it could be considered more broadly as a model for external cooperation.

All of these possible paths forward recognise that there are challenges at play from the law enforcement perspective in terms of the speed of access under MLA agreements. Yet remedying these challenges must be accomplished with a commitment to the rule of law and the proper safeguarding of privacy and the rights of defence for suspected persons.

4.2.2. Rights implications of prevention versus *ex post facto* law enforcement and law enforcement cooperation with security and intelligence services

Deterrence and prevention are important principles in cybercrime law enforcement practice, as shown in Europol's strategic analysis methodology used in iOCTA reporting for cybercrime threat analysis and strategic forecasts.[174] On the issue of deterrent approaches to cybercrime, a judicial participant at the 2015 Academy of European Law seminar pointed out that there is a mismatch between the growth of cybercrime and the 'static' caseload for courts, which he attributed to the focus on disruption rather than prosecution. In other words, if the right tools are not put in place, law enforcement authorities may operate "outside the law" out of necessity.[175] There are parallels here with the pre-emptive stance of counter-terrorism programmes, which often have ambitions to act before attacks occur following similar modes of strategic analysis and threat forecasting. While there is no inherent risk to rights in such threat forecasting, there are potential concerns related to profiling and interventions in advance of criminal acts. There is by now a large body of work in the field of counter-terrorism considering how this **pre-emptive principle impacts fundamental rights when individuals become subjects of law enforcement interest and intervention without being suspected or charged with crimes under standard legal frameworks**. Primary concerns include the speculative nature of the work, operation outside of existing legal frameworks, using intelligence as evidence, and, thus, lack of defence access to evidence used to justify interventions.[176]

While cybercrime is and should be considered as a different area of concern from a policy and legal perspective, it is worth considering how similar concerns might apply in this area,

[174] L. Buono (2014). 'Fighting Cybercrime through Prevention, Outreach, and Awareness Raising', *ERA Forum*, 15(1), 1-8. See also European Cybercrime Centre, 'The Internet Organised Crime Threat Assessment'.
[175] ERA Seminar on Countering the Illegal Use of the Internet (2015).
[176] For more on the legal landscape of pre-emption and fundamental rights, see V. Mitsilegas (2015), 'The Transformation of Privacy in an Era of Preemptive Surveillance', *Tilburg Law Review*, 20, 35-57.

particularly since the link between personal data processing and counter-terrorism is well established.[177] As previously discussed, definitions of cybercrime are a matter of competition between the domains and responsibilities of the police, security services and intelligence agencies. This can have significant implications for rights to privacy and data protection in cybercrime law enforcement activities. This potential to 'operate outside the law' should be a key question for fundamental rights in the realm of cybercrime, particularly when considering repeated references to the inadequacy of existing legal frameworks for cyber law enforcement cooperation and an emphasis on the need for new and faster modes of law enforcement and judicial cooperation and coordination. This raises questions about the legal structures for cross-border law enforcement utilising speculative, forecasting models in quickly changing technological environments. **Rights to non-discrimination should be considered alongside attention to rights to privacy and data protection in cyber law enforcement.** This is particularly important when only specific groups might be targeted, such as in the fields of counter-terrorism or counter-radicalisation.

4.2.3. Current context of the reform package on data protection

The above-mentioned challenges gain specific resonance in the context of the proposed European GDPR, meant to replace the Data Protection Directive (Directive 95/46/EC). The proposed Regulation aims to harmonise data protection regulations throughout the EU and extend EU data protection law to all companies processing the data of EU residents. Positioned within the Commission's prioritisation of the 'Digital Single Market', the GDPR is concerned, in part, with the goal of streamlining the regulatory environment for businesses. In parallel with the proposal for a GDPR, the Commission has set out a **proposed Directive on data processing for law enforcement purposes**. This Directive is intended to replace the 2008 Data Protection Framework Decision, which has several drawbacks: it focusses only on cross-border data processing, not on national processing; it has been implemented differently across Member States; no mechanism or advisory group supports common interpretations of its provisions; and the Commission lacks common implementation powers. The new Directive is intended to establish 'harmonised rules for the protection and the free movement of personal data in the areas of judicial cooperation in criminal matters and police cooperation'.[178] In March 2014 the EP adopted a compromise text on the proposed GDPR and the proposed Directive. The trilogue talks began in June 2015 and will continue throughout the year in an effort to come to an agreement on a final version of the Regulation.

Within this context, there are two particularly important things to note concerning possible implications for cybercrime law enforcement and rights to privacy and data protection. First, the Regulation broadly seeks to establish a single set of rules, a single point of contact, and one data protection authority ('a one-stop-shop') for businesses and individuals applicable across the EU. Yet the Regulation does not cover law enforcement cooperation. In the 2013 European Parliament report on the proposed Regulation, Rapporteur Jan Philipp Albrecht stated that he 'strongly regretted' that the European

[177] See, for example, the comments of Sir David Omand, former intelligence and security coordinator for the UK government on the role of personal data in preemptive counter-terrorism: 'Access to such [personal] information and in some cases the ability to apply data mining and pattern recognition software to databases, might well be the key to effective pre-emption in future terrorist cases'. See D. Omand (2009), *The National Security Strategy: Implications for the UK Intelligence Community*, London: Institute for Public Policy Research.

[178] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25 January 2012, Brussels.

Commission's proposed Regulation failed to cover law enforcement cooperation: '**This leaves legal uncertainty as regards rights and obligation (sic) in borderline issues, for instance where commercial data is accessed by law enforcement authorities for law enforcement purposes and transfers between authorities that are responsible for law enforcement and those that are not**'.[179] The current draft Regulation also states that it covers neither issues concerning fundamental rights and the flow of data in issues of national security nor activities undertaken in relation to the EU common foreign and security policy.[180] This could have implications for cybercrime law enforcement since cybercrime and cybersecurity can become blurred in practice, as detailed earlier. Thus, in a possible future 'streamlined' context**, the potential for continued 'legal uncertainty' is still at issue in cyber law enforcement**.

Second, the Regulation proposals aim to strip down the process of transferring data within and out of the EU by, for example, eliminating notification obligations. The current draft proposals suggest that international cooperation would be facilitated through 'adequacy decisions' taken at the European level. This acknowledges that a given non-EU country can guarantee adequate levels of data protection through its domestic laws or international commitments. This would apply in the business sector and in law enforcement to 'streamline' information flows between EU and non-EU countries. However, questions have been raised concerning the relevance of the 'adequate protection' approach and ambiguities in its application. At the Council, Member States' delegations questioned whether the adequacy approach would be 'emptied of meaning' when taking into account the 'manifold exceptions' in the draft Regulation, and whether it was appropriate given the potential for practical and political difficulties, such as negative adequacy decisions, and whether the approach would be feasible given the volume of data flows in cloud computing.[181] The recent ECJ Ruling on the Safe Harbour Agreement is interesting in that regard: The Court declared the Safe Harbour Decision invalid on the grounds that the US does not afford an adequate level of protection of personal data for EU citizens[182].

In March 2014 the European Parliament adopted a legislative resolution proposing to amend the draft Data Protection Directive's provisions on requirements applicable to data transfers or disclosures for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties of data initially processed for other purposes.[183] A recent policy study points out that the proposed article (43a) has implications for data disclosure outside Mutual Legal Assistance Treaties and other international agreements: 'The position adopted by the European Parliament thus accepts the possibility that a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data outside mutual legal assistance treaties or other international agreements, but conditions acceptance of such requests to a prior authorisation by a supervisory authority'.[184]

Thus, it should be noted that, **while the broad emphasis is on streamlining a comprehensive approach, uncertainties remain about how data protection**

[179] Explanatory Statement of Report of 22 November 2013 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 –C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht.

[180] See at http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf, 9.

[181] Council of the EU, Note on Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 9398/15, Brussels, 1 June 2015, 181.

[182] Court of Justice of the European Union, Judgment in Case C-362/14, Maximillian Schrems v Data Protection Commissioner, Luxembourg, 6 October 2015

[183] Article 43(a) was proposed in the 2014 legislative resolution adopted by the European Parliament on the proposed General Data Protection Regulation.

[184] Carrera, González Fuster, Guild, and Mitsilegas, *Access to Electronic Data*, 41.

safeguards will operate at the borders of different sectors and with third countries. The June 2015 compromise text on the Regulation, submitted for approval to the Council in order to engage in negotiations with representatives of the European Parliament, included the addition that the Regulation contains 'a margin of manoeuvre' for Member States where 'sector-specific laws that Member States have issued implementing Directive 95/46/EC should be able to be upheld'.[185]

5. GENERAL CONCLUSIONS AND RECOMMENDATIONS

This Study argues that debates on the law enforcement challenges of cybercrime in the EU should not be distracted by misleading discussions over encryption and claims over law enforcement 'going dark'. Rather, it shows that the key challenge for law enforcement is designing a sound legal and operational framework that guarantees the fundamental rights principles enshrined in EU primary and secondary law. This is critical to ensure due process and the successful prosecution of cybercriminal offences.

While recognising that some aspects of cybercrime (such as the reliance on specific digital tools for illicit activities and the conduct of such activities online) make investigations and prosecutions more difficult, **the Study underlines that one of the main challenges is the availability or development of specific technical skills to ensure proper forensic work** rather than counterproductive claims of the need for extraordinary means, such as the imposition of backdoors to encryption systems.

Another main challenge this Study analyses concerns the difficulties of carrying out investigations in multiple jurisdictions. While there is undoubtedly room for improvement in some of the main cooperation instruments (such as Mutual Legal Agreements), **the main risk is the development of operational arrangements with unmediated access outside legal channels**. Circumventing existing internal and external judicial and law enforcement cooperation commitments would pose significant challenges to the rule of law and fundamental rights. It would also run the risk of fuelling mistrust in transatlantic relations and among the general public.

Furthermore, the Study underlines the fact that much of the EU's policy on fighting cybercrime is based on non-legislative measures including operational cooperation and ad hoc public-private partnerships. **Given the complexity of the EU cybercrime infrastructure, the EP is largely excluded from policy developments in this field, impeding public scrutiny and accountability**. This compounds the EP's existing problems in ensuring that fundamental rights and data protection are diligently protected in the area of justice and home affairs.

The following recommendations aim at addressing these challenges:

Recommendation 1: The European Parliament should demand a review of EU cybercrime infrastructure and powers

As described throughout this Study, cross-border investigations and joint operations have minimal political or judicial oversight at the EU level. Although the European Parliament is the co-legislator in many of these areas, it risks being marginalised altogether with respect

[185] See at http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf, 7.

to the implementation and review of these policies by the exercise of delegated powers, EU agency discretion and non-legislative decision-making bodies.

Close monitoring of EU council structures, such as COSI, is particularly needed. The mechanisms through which the EP and national parliaments are kept 'informed' and how their comments can be taken into account must be a priority for the EP in relation to operational cybercrime cooperation matters. Such mechanisms could draw on TFEU Article 70 on impartial evaluation of EU policies, TFEU Article 71 on COSI and Article 6(2) of the COSI Decision.

Furthermore, the right to request at any time that a representative of Europol appear before the EP allows MEPs to ask questions and to stage debates when appropriate. **This right should be used more frequently and should cover the activities carried out by EC3, and in particular its Joint Cybercrime Action Taskforce (J-CAT)**. In a context where the EP is awaiting the Council's first reading position on the proposal for a Europol Regulation, under which the EU agency would have increased resources to further develop EC3, further information should be requested on the operational aspects of J-CAT, such as a detailed mapping of the liaison officers, their affiliations and their respective roles, as well as the forms of coordination and cooperation they carry out.

Finally, and related to joint operational activities of the EU with third countries, Europol and Eurojust have the power to conclude agreements with third countries and other international organisations that concern the exchange of information and personal data. If the content of these agreements is assessed by their respective Joint Supervisory Boards, **the transparency of the negotiating process should be improved further**. For instance, these agreements could be published in the Official Journal, opening up possibilities for improved accountability and access to justice.

The EP should demand a review that ultimately seeks to **codify what is presently an extremely complicated mash-up of legislative and non-legislative measures** in order to make clear to citizens who does what, why, and how in the cybercrime area - with the aim of instituting further accountability and transparency.

The EP should also demand that the modus operandi for **all public-private partnerships in the area of cybercrime are subject to open review and public debate**, and placed on a formal legal footing with attendant fundamental rights guarantees.

Recommendation 2: The European Parliament should ensure that the development of any cooperation/information-sharing framework guarantees rights

Third-country access to data outside MLA agreements is problematic, raising particular concern regarding the US, not least because of the differences in EU and US approaches to data protection and the lack of effective judicial privacy protection afforded to EU citizens on US territory. The forthcoming consent procedure on the EU-US data protection 'Umbrella agreement' will provide an opportunity for the EP to review the provisions of the agreement and ensure they provide sufficient safeguards as to the lawfulness of data transfers.

Any future cooperation arrangements should **stipulate clear limits to judicial cooperation on both human rights and proportionality grounds,** as laid down in the European Investigation Order (EIO) that will become the principal instrument governing evidence exchange and mutual legal assistance between Member States. The fact that human rights safeguards enshrined in the EIO will also constitute benchmarks for the external action of the EU and Member States in the field is a welcome step.

In the context of the current data protection reform package, while the broad emphasis is on streamlining a comprehensive approach, uncertainties remain about how data protection safeguards will operate at the intersection of different sectors and with third countries. Therefore, an updated legal framework designed to overcome the cooperation challenge should foreground fundamental rights concerns. This is essential to ensuring due process and the successful prosecution of cybercriminal offences.

Recommendation 3: The European Parliament should ensure that the CoE Cybercrime Convention's obligations on Member States are consistent with EU law and fundamental rights protections

Discussions on a revised Convention have raised the possibility of unmediated transnational access to data outside of MLA agreements. The Cybercrime Convention Committee has put forward controversial proposals aimed at amending Article 32, which concerns trans-border access to stored computer data. **It is thus of crucial importance that the details of any such protocols should be drafted in consultation with the EP and that the rule of law and respect for EU fundamental rights be ensured**.

Recommendation 4: The European Parliament must ensure that cybercrime is not used as a justification to undermine new information security protocols and the right to privacy in telecommunications

Cybercrime is often presented as a challenge that requires actions against a new generation of encrypted communication services available to citizens and businesses. In light of the numerous problems raised by encryption and 'exceptional access' analysed in the Study, **the EP must ensure that cybercrime is not used as a justification to undermine new information security protocols and the right to privacy in telecommunications,** which are a fundamental component of the Internet's functioning and future development.

Recommendation 5: CEPOL should ensure that training courses on cybercrime forensics and digital evidence include an applied fundamental rights component.

The fast pace of technological change and the evolving methods employed by cybercriminals clearly mean that law enforcement agencies have to enhance their knowledge and skills. Central elements in this are improving capacity on cybercrime forensics and gathering and handling digital evidence. There is clearly a role for CEPOL to provide EU-wide support in this regard. However, as the findings of this Study have made clear, it is imperative that new techniques and investigative methods are disseminated and used **in full compliance with the EU Charter of Fundamental Rights**.

REFERENCES

Academic references:

Abelson, H. et al. (1997), 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption', New York, NY: Columbia University Academic Commons.

Abelson, H. et al. (2015), *Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Cambridge, MA: Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report, No. 26, 6 July.

Adrian, D. et al. (2015), 'Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice,' 20 May.

Allison, G. T. (1971), *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little Brown.

Anderson, M. et al. (1996), *Policing the European Union*, Oxford: Oxford University Press.

Bigo, D. (1996), *Polices en réseaux: L'Expérience européenne*, Paris: Presses de la Fondation Nationale des Sciences Politiques.

_______ (2010), 'Freedom and Speed in Enlarged Borderzones', in V. Squire (ed.), *The Contested Politics of Mobility: Borderzones and Irregularity*, London: Routledge.

Bigo, D. et al. (2012), 'Fighting Cyber Crime and Protecting Privacy in the Cloud', Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), PE 462.509, Brussels.

Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. and Scherrer, A. (2013), *National programmes for mass surveillance of personal data by EU Member States and their compatibility with EU Law*, Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), PE 493.032, Brussels.

Broadhurst, R. et al. (2014), 'Organizations and Cybercrime: An Analysis of the Nature of Groups Engaged in Cybercrime', *International Journal of Cyber Criminology*, 8(1), 1-20.

Buono, L. (2014). 'Fighting Cybercrime through Prevention, Outreach, and Awareness Raising', *ERA Forum*, 15(1), 1-8.

Carrera, S., González Fuster, G., Guild, E. and Mitsilegas, V. (2015), *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*, Brussels: Centre for European Policy Studies

Cohen, S. (2002) [1972], *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, London: Routledge, 3rd edition.

Cole, S. A. and Pontell, H. D. (2006), '"Don't Be Low Hanging Fruit": Identity Theft as Moral Panic', in Torin Monahan (ed.), *Surveillance and Security: Technological Politics and Power in Everyday Life*, London: Routledge, 125-148.

Den Boer, M. (1998), 'Wearing the Inside Out: European Police Cooperation Between Internal and External Security', *European Foreign Affairs Review*, 2(4), 491–508.

Dam, K. W. and Lin, H. S. (eds.) (1996), *Cryptography's Role in Securing the Information Society*, Washington, D.C.: National Academies Press.

Giacomello, G. (2002), *National Governments and Control of the Internet: A Digital Challenge*, London: Routledge.

Goode, E., and Ben-Yehuda, N. (2009) [1994], *Moral Panics: The Social Construction of Deviance*, Oxford: Wiley-Blackwell.

Herrmann, R. K. and Lebow, R. N., (2004) *Ending the Cold War: Interpretations, Causation, and the Study of International Relations*, Basingstoke: Palgrave Macmillan.

Hollinger, R., and Lanza-Kaduce, L. (1988), 'The Process of Criminalization: The Case of Computer Crime Laws', *Criminology*, 26(1), 101-126.

Korff, D. (2014), 'Rule of Law on the Internet and in the Wider Digital World', Council of Europe Commissioner for Human Rights Issue Paper, 12.

Levy, S. (1993), 'Crypto Rebels', *Wired Magazine*, 1(2), May/June.

Lusthaus, J. (2013), 'How Organized Is Organized Cybercrime?', *Global Crime*, 14(1), 52-60.

MacLaughlin, E., and Muncie, J. (2013), *The SAGE Dictionary of Criminology,* London: SAGE.

Mitsilegas, V. (2015), 'The Transformation of Privacy in an Era of Preemptive Surveillance', *Tilburg Law Review*, 20, 35-57.

O'Brien, D. (2006), 'The World's Worst Internet Law Sneaking Through the Senate', *Electronic Frontier Foundation*, 3 August.

Omand, D. (2009), *The National Security Strategy: Implications for the UK intelligence community*, London: Institute for Public Policy Research.

Rodriguez, K. (2011), 'Dangerous Cybercrime Treaty Pushes Surveillance and Secrecy Worldwide', *Electronic Frontier Foundation*, 25 August.

Scherrer, A., Jeandesboz, J. and Guittet, E.-P. (2010), *Developing an EU Internal Security Strategy, Fighting Terrorism and Organised Crime*, Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), PE 462.423, Brussels.

Sommer, P. (2006), 'Criminalising Hacking Tools', *Digital Investigation*, 3(2), 68-72

Zalnieriute, M. and Schneider, T. (2014), *ICANN's Procedures and Policies in the Light of Human Rights, Fundamental Freedoms and Democratic Values*, Council of Europe Report, DGI(2014)12.

Official sources:

Agreement on mutual legal assistance between the European Union and the United States of America (OJ L 2003 181/34)

Committee on Civil Liberties, Justice and Home Affairs (2013), Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Rapporteur: Jan Philipp Albrecht.

Council of Europe (2001), Convention on Cybercrime, CETS No. 185: Budapest, 23 November 2001

Council of Europe (2015), Positions on counter-terrorism and human rights protection, Council of Europe CommDH Position Paper

Decision of 6 December 2001, extending Europol's mandate to deal with the serious forms of international crime listed in the Annex to the Europol Convention

Decision of 12 February 2007 establishing for the period 2007-2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention of and Fight against Crime'

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Annulled by Judgment in Case number C-293/12, Court of Justice of the European Union, 8 April 2014)

Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters

ENISA (2014), Threat Landscape 2014: Overview of current and emerging cyber-threats, December 2014

ENISA (2014), 'Fighting Cybercrime: Strategic Cooperation Agreement Signed between ENISA and Europol', press release, 6 June 2014

EU Council (2008), Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime, 2987th Justice and Home Affairs Council meeting, Brussels, 27-28 November 2008

EU Council (2008), Revised EU Radicalisation and Recruitment Action Plan, Doc.15244/08 EXT 1, 14 November 2008

EU Council (2009), Conclusions on the European Financial Coalition and national financial coalitions against child pornography on the Internet, 2969th Justice and Home Affairs Council meeting, Luxembourg, 23 October 2009

EU Council (2009), Revised EU Radicalisation and Recruitment Action Plan, Doc.15374/09, 5 November 2009

EU Council (2010), Adoption of draft Council Conclusions on an Action Plan to implement the Concerted Strategy to combat cybercrime, Doc.8535/10, 16 April 2010

EU Council (2010), Conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime, 3010th General Affairs Council meeting, Luxembourg, 26 April 2010

EU Council (2010), Conclusions on the use of a standardised, multidimensional semi-structured instrument for collecting data and information on the processes of radicalisation in the EU, 3010th General Affairs Council meeting, Luxembourg, 26 April 2010

EU Council (2011), Combating sexual exploitation of children and child pornography on the Internet - strengthening the effectiveness of police activities in the EU Member States - Results of questionnaire, Doc.16069/11, 26 October 2011

EU Council (2011), Implementation EU Policy cycle for organised and serious international crime: Draft strategic goals related to the EU crime priority 'Cybercrime and the criminal misuse of the internet', Doc.14452/2/11, 17 October 2011

EU Council (2014), EU Cyber Defence Policy Framework, Brussels 15585/14, 18 November 2014

EU Council (2014), Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism, Doc.9956/14, 19 May 2014

EU Council (2015), Combating terrorism and radicalisation: further strengthening the protection of the citizens of the European Union, Doc.5507/15, 23 January 2015

EU Council (2015), Note on Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 9398/15, Brussels, 1 June 2015

EU Council (2015), Outcome of the CEPOL - Presidency conference on cybercrime: Strategic Approach on Cybercrime. Future Challenges in Tackling Online Criminality, 25-27 March 2015, Jūrmala, Latvia, Doc. 7368/15, 8 April 2015

EU Council (2015), Preventing Radicalisation and Recruitment to Terrorist Groups, Doc.10916/05, 15 May 2015

European Central Bank (2015), Virtual currency schemes – a further analysis, Frankfurt: European Central Bank

European Commission (2001), Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by improving the Security of Information Infrastructures and Combating Computer-related Crime. Brussels, COM(2001) 890 final, 26 January

European Commission (2007), Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime, Brussels, COM(2007) 267 final, 22.5.2007

European Commission (2009), Commission Delegated Regulation of 22.10.2014 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items

European Commission (2010), Communication on a comprehensive approach on personal data protection in the European Union, COM(2010)609 final, 4 November 2010

European Commission (2011), Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security', Brussels, COM(2011) 163 final, 31 March 2011

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

European Commission (2012), Declaration on the Launch of the Global Alliance against child sexual abuse online, Brussels, 5 December 2012

European Commission (2012), Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25 January 2012, Brussels

European Commission (2012), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels, COM(2012) 11 final, 25 January

European Commission (2012), Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final, Brussels, 25 January 2012

European Commission (2012), Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25 January 2012, Brussels

European Commission (2013), Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace, Brussels, JOIN(2013) 1 final, 7 April

European Commission (2013), EU Cyber Security Strategy – open, safe and secure, Communication, JOIN(2013) 1 final

European Commission (2013), 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. Brussels, COM (2013) 173 final, 27 March

European Commission (2013), Rebuilding Trust in EU-US Data Flows, COM/2013/0846 final

European Commission (2014), Joint statement Malmström - Alfano on the informal ministerial dinner with IT companies, Luxembourg, 9 October 2014

European Commission (2015), Fact Sheet, Questions and Answers on the EU-US data protection ‘Umbrella agreement’, Brussels, 8 September 2015

European Commission (2015), The European Agenda on Security, Brussels, COM(2015) 185 final, 28 April

European Court of Justice (2014), Judgement in Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014

European Court of Justice, Judgment in Case C-362/14, Maximillian Schrems v Data Protection Commissioner, Luxembourg, 6 October 2015

European Cybercrime Centre (2014), ‘First Year Report’, The Hague: Europol

European Data Protection Supervisor (2012), Opinion on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre, Doc. 12406/12, 10 July 2012

Europol (2014), ‘Cybercrime Experts Tackle the Criminal Exploitation of Virtual Currencies’, press release, 17 June 2014

Europol (2014), ‘Massive Changes in the Criminal Landscape’, press release, 17 June 2014

Europol (2014), The Internet Organised Crime Threat Assessment (iOCTA), The Hague: Europol

Europol (2015), The Internet Organised Crime Threat Assessment (iOCTA), The Hague:

Europol

Europol (2015), 'Botnet Taken Down through International Law Enforcement Cooperation', press release, 25 February 2015

Europol (2015), 'Europol's Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda', press release, 1 July 2015

Europol (2015), 'International Operation Dismantles Criminal Group of Cyber-Fraudsters', press release, 10 June 2015,

Europol (2015), 'Mandate of Joint Cybercrime Action Taskforce Extended after Successful First Six Months', press release, 24 June 2015

Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment

Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography

Framework Decision 2005/222/JHA on attacks against information systems

Regulation 460/2004/EC of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency

Regulation 526/2013/EU of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

ANNEX: List of Interviews

For the purpose of this Study, the following interviews were conducted:

Eurojust:

Koen Hermans, Prosecutor, Assistant to the National Member for the Netherlands

Europol (EC3):

Fernando Ruiz, Acting Head of Operations
Jaap van Oss, Focal Point Manager FP CYBORG – Intrusion, Malwares
Philip Aman, Senior Strategic Analyst, Team Leader Strategy and Development
Aglika Klayn, Strategy and Development
Gregory Mounier, Strategy and External Relations

Centre for Democracy and Technology (CDT, Brussels):

Jens-Henrick Jeppesen, Representative and Director for European Affairs

Access, Mobilizing for Global Digital Freedom:

Amie Stepanovich, US Policy Manager

CAT: QA-04-15-764-EN-C (paper)
CAT: QA-04-15-764-EN-N (pdf)

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- ■ Constitutional Affairs
- ■ Justice, Freedom and Security
- ■ Gender Equality
- ■ Legal and Parliamentary Affairs
- ■ Petitions

Documents

Visit the European Parliament website:
http://www.europarl.europa.eu/supporting-analyses

PHOTO CREDIT: iStock International Inc.

ISBN 978-92-823-8297-4 (paper)
ISBN 978-92-823-8298-1 (pdf)

doi: 10.2861/996881 (paper)
doi: 10.2861/438776 (pdf)

Publications Office