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

Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices

STUDY FOR THE LIBE COMMITTEE

EN

2017

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Legal Frameworks for Hacking by Law Enforcement:

Identification, Evaluation and Comparison of Practices

STUDY

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, presents concrete policy proposals on the use of hacking techniques by law enforcement. These proposals are driven by a comparative examination of the legal frameworks for hacking by law enforcement across six EU Member States and three non-EU countries, in combination with analyses of the international and EU-level debates on the topic and the EU legal basis for intervention in the field.

PE 583.137 EN

ABOUT THE PUBLICATION

This research paper was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and was commissioned, overseen and published by the Policy Department for Citizens' Rights and Constitutional Affairs.

Policy Departments provide independent expertise, both in-house and externally, to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU external and internal policies.

To contact the Policy Department for Citizens' Rights and Constitutional Affairs or to subscribe to its newsletter please write to:
poldep-citizens@ep.europa.eu

Research Administrator Responsible

Kristiina MILT
Policy Department C: Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@ep.europa.eu

AUTHORS

Mirja GUTHEIL, Optimity Advisors
Quentin LIGER, Optimity Advisors
Aurélie HEETMAN, Optimity Advisors
James EAGER, Optimity Advisors
Max CRAWFORD, Optimity Advisors

With the support of Professor Bert-Jaap KOOPS and Ivan SKORVÁNEK of the Tilburg Institute for Law, Technology, and Society (TILT) at Tilburg University; Carly NYST, independent expert; Gerben KLEIN BALTINK, Chairman of the Dutch Internet Standards Platform; and Professor Catherine CRUMP, Assistant Clinical Professor of Law and Acting Director of the Samuelson Law, Technology & Public Policy Clinic, University of California.

LINGUISTIC VERSIONS

Original: EN

Manuscript completed in March 2017

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

ABW	Internal Security Agency (Poland)
ACLU	American Civil Liberties Union
AIVD	General Intelligence & Security Service (the Netherlands)
BKAG	Federal Criminal Police Act (Germany)
CALEA	US Communications Assistance for Law Enforcement Act 1994
CCITÜ	Competence Centre for Information Technological Surveillance (Germany)
CCPCJ	UN Commission for Crime Prevention and Criminal Justice
CoE	Council of Europe
DUCG	Dual-Use Coordination Group
EC3	European Cybercrime Centre – Europol
ECHR	European Convention on Human Rights
ECPA	Electronic Communications Act (US)
EDPS	European Data Protection Supervisor
EFF	Electronic Frontier Foundation
ENISA	European Union Agency for Network and Information Security
EWG	Encryption Working Group (US)
FBI	Federal Bureau of Investigation (US)
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology

Interpol	International Criminal Police Organisation
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
LIBE Committee	European Parliament Committee on Civil Liberties, Justice and Home Affairs
MIVD	Military Intelligence & Security Service (the Netherlands)
NCA	National Crime Agency (UK)
NDA	Non-Disclosure Agreement
NGO	Non-Governmental Organisation
NIT	Network Investigative Technique
NSA	National Security Agency (US)
SCA	Stored Communications Act (US)
STEG	Surveillance Technology Expert Group
StPO	Code of Criminal Procedure (Germany)
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
Tor	The Onion Router
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
VEP	Vulnerability Equities Process
VPN	Virtual Private Networks
ZITiS	Central Office for Information in the Security Sphere (Germany)

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Hacking by law enforcement is a relatively new phenomenon within the framework of the longstanding public policy problem of balancing security and privacy. On the one hand, law enforcement agencies assert that the use of hacking techniques brings security, stating that it represents a part of the solution to the law enforcement challenge of encryption and 'Going Dark' without systematically weakening encryption through the introduction of 'backdoors' or similar techniques. On the other hand, civil society actors argue that hacking is extremely invasive and significantly restricts the fundamental right to privacy. Furthermore, the use of hacking practices pits security against cybersecurity, as the exploitation of cybersecurity vulnerabilities to provide law enforcement with access to certain data can have significant implications for the security of the internet.

Against this backdrop, the present study provides the LIBE Committee with relevant, actionable insight into the legal frameworks and practices for hacking by law enforcement. Firstly, the study examines the **international and EU-level debates** on the topic of hacking by law enforcement (**Chapter 2**), before analysing the **possible legal bases for EU intervention** in the field (**Chapter 3**). These chapters set the scene for the primary focus of the study: the **comparative analysis of legal frameworks and practices for hacking by law enforcement** across six selected Member States (France, Germany, Italy, the Netherlands, Poland and the UK), with further illustrative examples from three non-EU countries (Australia, Israel and the US) (**Chapter 4**). Based on these analyses, the study **concludes** (**Chapter 5**) and presents concrete **recommendations and policy proposals** for EU action in the field (**Chapter 6**).

The **international and EU-level debates** on the use of hacking techniques by law enforcement primarily evolve from the law enforcement challenge posed by encryption – i.e. the 'Going Dark' issue.

'Going Dark' *is a term used "to describe [the] decreasing ability [of law enforcement agencies] to lawfully access and examine evidence at rest on devices and evidence in motion across communications networks".*[1]

According to the International Association of Chiefs of Police (IACP), law enforcement agencies are not able to investigate illegal activity and prosecute criminals without this evidence. Encryption technologies are cited as one of the major barriers to this access. Although recent political statements from several countries (including France, Germany, the UK and the US) seemingly call for 'backdoors' to encryption technologies, support for strong encryption at international and EU fora remains strong. As such, law enforcement agencies across the world started to use hacking techniques to bypass encryption. Although the term 'hacking' is not used by law enforcement agencies, these practices essentially mirror the techniques used by hackers (i.e. exploiting any possible vulnerabilities – including technical, system and/or human vulnerabilities – within an information technology (IT) system).

Law enforcement representatives, such as the IACP and Europol, report that access to encrypted and other data through such hacking techniques brings significant investigative benefits. However, it is not the only possible law enforcement solution to the 'Going Dark' issue. Outside of the scope of this study, the other options include: requiring users to provide their password or decrypt their data; requiring technology vendors and service providers to bypass the security of their own products and services; and the systematic weakening of

[1] IACP Summit Report. 2015. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence.

encryption through the mandated introduction of 'backdoors' and/or weakened standards for encryption.

With the benefits of hacking established, a 2016 Joint Statement published by the European Union Agency for Network and Information Security (ENISA) and Europol[2] noted that the use of hacking techniques also brings several key risks.

The primary risk relates to the **fundamental right to privacy** and freedom of expression and information, as enshrined in international, EU and national-level law. Hacking techniques are extremely invasive, particularly when compared with traditionally intrusive investigative tools (e.g. wiretapping, house searches etc.). Through hacking, law enforcement can gain access to all data stored or in transit from a device; this represents a significant amount of data (e.g. a recent investigation by Dutch law enforcement collected seven terabytes of data, which translates into around 86 million pages of Microsoft Word documents[3]), as well as extremely sensitive data (e.g. a person's location and movements, all communications, all stored data etc.). Consequently, **the use of hacking techniques will inherently restrict the fundamental right to privacy**.

Therefore, current debates at international and EU fora focus on assessing and providing recommendations on the current legal balances and safeguards for the restriction of the right to privacy by hacking techniques. However, these debates have assumed that hacking practices are necessary for law enforcement and simply require governing laws; they have not discussed whether the use of hacking techniques by law enforcement is necessary and proportional. The law enforcement assertions regarding the necessity of these invasive tools have not been challenged.

The second key risk relates to the **security of the internet**. Law enforcement use of hacking techniques has the potential to significantly weaken the security of the internet by "[increasing] the attack surface for malicious abuse"[4]. Given that critical infrastructure and defence organisations, as well as law enforcement agencies themselves, use the technologies targeted and potentially weakened by law enforcement hacking, the potential ramifications reach far beyond the intended target.

As such, debates at international and EU fora focus on the appropriate balances between security and privacy, as well as security and cybersecurity. Regarding **security v. privacy**, the debates to date have assessed and provided recommendations on the legislative safeguards required to ensure that hacking techniques are only permitted in situations where a restriction of the fundamental right to privacy is valid in line with EU legislation (i.e. legal, necessary and proportional). Regarding **security v. cybersecurity**, the debates have been limited and primarily centre around the use and/or reporting of zero-day vulnerabilities discovered by law enforcement agencies.

Further risks not discussed in the Joint Statement but covered by this study include: the risks to **territorial sovereignty** – as law enforcement agencies may not know the physical location of the target data; and the risks related to the **supply and use of commercially-developed hacking tools by governments with poor consideration for human rights**.

Alongside the analysis of international and EU debates, the study presents hypotheses on the legal bases for EU intervention in the field. Although possibilities for EU legal intervention in

[2] ENISA and Europol. 2016. On lawful criminal investigation that respects the 21st Century data protection. Europol and ENISA Joint Statement.

[3] Paganini, P. 2017. Ennetcom – Dutch Police confirmed to have decrypted BlackBerry PGP messages in a criminal case. Article on Security Affairs, 10 March 2017.

[4] ENISA and Europol. 2016. On lawful criminal investigation that respects the 21st Century data protection. Europol and ENISA Joint Statement.

several areas are discussed, including mutual admissibility of evidence (Art. 82(2) TFEU), common investigative techniques (Art. 87(2)(c) TFEU), operational cooperation (Art. 87(3) TFEU) and data protection (Art. 16 TFEU, Art. 7 & 8 EU Charter), the onus regarding the development of legislation in the field is with the Member States. As such, the management of the risks associated with law enforcement activities is governed at the Member State level.

As suggested by the focus of the international and EU discussions, concrete measures need to be stipulated at national-level to manage these risks. This study presents a comparative analysis of the legal frameworks for hacking by law enforcement across six Member States, as well as certain practical aspects of hacking by law enforcement, thereby providing an overview of the primary Member State mechanisms for the management of these risks. Further illustrative examples are provided from research conducted in three non-EU countries.

More specifically, the study examines the **legal and practical balances and safeguards implemented at national-level** to ensure: i) the legality, necessity and proportionality of restrictions to the fundamental right to privacy; and ii) the security of the internet.

Regarding restrictions to the right to privacy, the study first examines the existence of specific legal frameworks for hacking by law enforcement, before exploring the *ex-ante* and *ex-post* conditions and mechanisms stipulated to govern restrictions of the right to privacy and ensure they are legal, necessary and proportional.

It is found that hacking practices are seemingly necessary across all Member States examined, as **four Member States (France, Germany, Poland and the UK) have adopted specific legislative provisions and the remaining two are in the legislative process**. For all Member States except Germany, the adoption of specific legislative provisions occurred in 2016 (France, Poland and the UK) or will occur later (Italy, the Netherlands). This confirms the new nature of these investigative techniques.

Additionally, law enforcement agencies in all Member States examined have used, or still use, hacking techniques in the absence of specific legislative provisions, under so-called 'grey area' legal provisions. Given the invasiveness of hacking techniques, these **'grey area' provisions are considered insufficient to adequately protect the right to privacy.**

Where specific legal provisions have been adopted, all stakeholders agree that a restriction of the right to privacy requires the implementation of certain safeguards. The current or proposed legal frameworks of all six Member States comprise a suite of *ex-ante* conditions and *ex-post* mechanisms that aim to ensure the use of hacking techniques is proportionate and necessary. As recommended by various UN bodies, the provisions of primary importance include **judicial authorisation** of hacking practices, **safeguards** related to the nature, scope and duration of possible measures (e.g. limitations to crimes of a certain gravity and the duration of the hack, etc.) and independent **oversight**.

Although many of these types of recommended conditions are common across the Member States examined – demonstrated in the below table – their implementation parameters differ. For instance, both German and Polish law permit law enforcement hacking practices without judicial authorisation in exigent circumstance if judicial authorisation is achieved in a specified timeframe. However, the timeframe differs (three days in Germany compared with five days in Poland). These differences make significant difference, as the Polish timeframe was criticised by the Council of Europe's Venice Commission for being too long.[5]

[5] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016

Furthermore, the Member States examined all accompany these common types of *ex-ante* and *ex-post* conditions with different, less common conditions. This is particularly true for *ex-post* oversight mechanisms. For instance, in Poland, the Minister for internal affairs provides macro-level information to the lower (Sejm) and upper (Senat) chambers of Parliament;[6] and in the UK, oversight is provided by the Investigatory Powers Commissioner, who reviews all cases of hacking by law enforcement, and the Investigatory Powers Tribunal, which considers disputes or complaints surrounding law enforcement hacking.[7]

Key *ex-ante* considerations	
Judicial authorisation	The legal provisions of all six Member States require *ex-ante* judicial authorisation for law enforcement hacking. The information to be provided in these requests differ. Select Member States (e.g. Germany, Poland, the UK) also provide for hacking without prior judicial authorisation in exigent circumstances if judicial authorisation is subsequently provided. The timeframes for *ex-post* authorisation differ.
Limitation by crime and duration	All six Member States restrict the use of hacking tools based on the gravity of crimes. In some Member States, the legislation presents a specific list of crimes for which hacking is permitted; in others, the limit is set for crimes that have a maximum custodial sentence of greater than a certain number of years. The lists and numbers of years required differ by Member State. Many Member States also restrict the duration for which hacking may be used. This restriction ranges from maximum 1 month (France, Netherlands) to a maximum of 6 months (UK), although extensions are permitted under the same conditions in all Member States.
Key *ex-post* considerations	
Notification and effective remedy	Most Member States provide for the notification of targets of hacking practices and remedy in cases of unlawful hacking.
Reporting and oversight	Primarily, Member States report at a micro-level through logging hacking activities and reporting them in case files. However, some Member States (e.g. Germany, Poland and the UK) have macro-level review and oversight mechanisms.

Furthermore, as regards the issue of territoriality (i.e. the difficulty law enforcement agencies face obtaining the location of the data to be collected using hacking techniques), only one Member States, the Netherlands, legally permits the hacking of devices if the location is unknown. If the device turns out to be in another jurisdiction, Dutch law enforcement must apply for Mutual Legal Assistance.

As such, when aggregated, these provisions strongly mirror Article 8 of the European Convention on Human Rights, as well as the UN recommendations and paragraph 95 of the ECtHR judgement in Weber and Saravia v. Germany. However, there are many, and varied,

[6] Polish Act on the Police of 6 April 1990. Article 19 §22. Translation provided by the Council of Europe.

[7] Equipment Interference DRAFT Code of Practice, Autumn 2016. Oversight.

criticisms when the Member State conditions are examined in isolation. Some of the provisions criticised include: the limits based on the gravity of crimes (e.g. the Netherlands, France and Poland); the provisions for notification and effective remedy (e.g. Italy and the Netherlands); the process for screening and deleting non-relevant data (Germany); the definition of devices that can be targeted (e.g. the Netherlands); the duration permitted for hacking (e.g. Poland); and a lack of knowledge amongst the judiciary (e.g. France, Germany, Italy and the Netherlands).With this said, certain elements, taken in isolation, can be called good practices. Such examples are presented below.

Select good practice: Member State legislative frameworks

Germany: Although they were deemed unconstitutional in a 2016 ruling, the provisions for the screening and deletion of data related to the core area of private life are a positive step. If the provisions are amended, as stipulated in the ruling, to ensure screening by an independent body, they would provide strong protection for the targeted individual's private data.

Italy: The 2017 draft Italian law includes a range of provisions related to the development and monitoring of the continued use of hacking tools. As such, one academic stakeholder remarked that the drafting of the law must have been driven by technicians. However, these provisions bring significant benefits to the legislative provisions in terms of supervision and oversight of the use of hacking tools. Furthermore, the Italian draft law takes great care to separate the functionalities of the hacking tools, thus protecting against the overuse or abuse of a hacking tool's extensive capabilities.

Netherlands: The Dutch Computer Crime III Bill stipulates the need to conduct a formal proportionality assessment for each hacking request, with the assistance of a dedicated Central Review Commission (Centrale Toetsings Commissie). Also, the law requires rules to be laid down on the authorisation and expertise of the investigation officers that can perform hacking.

With these findings in mind, the study concludes that the **specific national-level legal provisions examined provide for the use of hacking techniques in a wide array of circumstances**. The varied combinations of requirements, including those related to the gravity of crimes, the duration and purpose of operations and the oversight, result in a situation where the law does not provide for much stricter conditions than are necessary for less intrusive investigative activities such as interception.

Based on the study findings, relevant and actionable **policy proposals and recommendations** have been developed under the two key elements: i) the fundamental right to privacy; and ii) the security of the internet.

Recommendations and policy proposals: Fundamental right to privacy

It is recommended that the use of 'grey area' legal provisions is not sufficient to protect the fundamental right to privacy. This is primarily because existing legal provisions do not provide for the more invasive nature of hacking techniques and do not provide for the legislative precision and clarity as required under the Charter and the ECHR.

Furthermore, many of these provisions have only recently been enacted. As such, there is a need for robust evidence-based monitoring and evaluation of the practical application of these provisions. It is therefore recommended that the application of these new legal provisions is evaluated regularly at national level, and that the results of these evaluations are assessed at EU-level.

If specific legislative provisions are deemed necessary, the study recommends a range of good practice, specific *ex-ante* and *ex-post* provisions governing the use of hacking practices by law enforcement agencies. These are detailed in Chapter 6.

Policy proposal 1: *The European Parliament should pass a resolution calling on Member States to conduct a Privacy Impact Assessment when new laws are proposed to permit and govern the use of hacking techniques by law enforcement agencies. This Privacy Impact Assessment should focus on the necessity and proportionality of the use of hacking tools and should require input from national data protection authorities.*

Policy proposal 2: *The European Parliament should reaffirm the need for Member States to adopt a clear and precise legal basis if law enforcement agencies are to use hacking techniques.*

Policy proposal 3: *The European Parliament should commission more research or encourage the European Commission or other bodies to conduct more research on the topic. In response to the Snowden revelations, the European Parliament called on the EU Agency for Fundamental Rights (FRA) to thoroughly research fundamental rights protection in the context of surveillance. A similar brief related to the legal frameworks governing the use of hacking techniques by law enforcement across all EU Member States would act as an invaluable piece of research.*

Policy proposal 4: *The European Parliament should encourage Member States to undertake evaluation and monitoring activities on the practical application of the new legislative provisions that permit hacking by law enforcement agencies.*

Policy proposal 5: *The European Parliament should call on the EU Agency for Fundamental Rights (FRA) to develop a practitioner handbook related to the governing of hacking by law enforcement. This handbook should be intended for lawyers, judges, prosecutors, law enforcement officers and others working with national authorities, as well as non-governmental organisations and other bodies confronted with legal questions in the areas set out by the handbook. These areas should cover the invasive nature of hacking techniques and relevant safeguards as per international and EU law and case law, as well as appropriate mechanisms for supervision and oversight.*

Policy proposal 6: *The European Parliament should call on EU bodies, such as the FRA, CEPOL and Eurojust, to provide training for national-level members of the judiciary and data protection authorities, in collaboration with the abovementioned handbook, on the technical means for hacking in use across the Member States, their potential for invasiveness and the principles of necessity and proportionality in relation to these technical means.*

Recommendations and policy proposals: Security of the internet

The primary recommendation related to the security of the internet is that the position of the EU against the implementation of 'backdoors' and similar techniques, and in support of strong encryption standards, should be reaffirmed, given the prominent role encryption plays in our society and its importance to the EU's Digital Agenda. To support this position, the EU should ensure continued engagement with global experts in computer science as well as civil society privacy and digital rights groups.

The actual impacts of hacking by law enforcement on the security of the internet are yet unknown. More work should be done at the Member State level to assess the potential impacts such that these data can feed in to overarching discussions on the necessity and proportionality of law enforcement hacking. Furthermore, more work should be done, beyond understanding the risks to the security of the internet, to educate those involved in the authorisation and use of hacking techniques by law enforcement.

At present, the steps taken to safeguard the security of the internet against the potential risks of hacking are not widespread. As such, the specific legislative provisions governing the use of hacking techniques by law enforcement, if deemed necessary, should safeguard the security of the internet and the security of the device, including reporting the vulnerabilities used to gain access to a device to the appropriate technology vendor or service provider; and ensure the full removal of the software or hardware from the targeted device.

Policy proposal 7: *The European Parliament should pass a resolution calling on Member States to conduct an Impact Assessment to examine the impact of new or existing laws governing the use of hacking techniques by law enforcement on the security of the internet.*

Policy proposal 8: *The European Parliament, through enhanced cooperation with Europol and the European Union Agency for Network and Information Security (ENISA), should reaffirm its commitment to strong encryption considering discussions on the topic of hacking by law enforcement. In addition, the Parliament should reaffirm its opposition to the implementation of 'backdoors' and similar techniques in information technology infrastructures or services.*

Policy proposal 9: *Given the lack of discussion around handling zero-day vulnerabilities, the European Parliament should support the efforts made under the* cybersecurity contractual Public-Private Partnership (PPP) *to develop appropriate responses to handling zero-day vulnerabilities, taking into consideration the risks related to fundamental rights and the security of the internet.*

Policy proposal 10: *Extending policy proposal 4, above, the proposed FRA handbook should also cover the risks posed to the security of the internet by using hacking techniques.*

Policy proposal 11: *Extending policy proposal 5, training provided to the judiciary by EU bodies such as FRA, CEPOL and Eurojust should also educate these individuals on the risks posed to the security of the internet by hacking techniques.*

Policy proposal 12: *Given the lack of discussion around the risks posed to the security of the internet by hacking practices, the European Parliament should encourage debates at the appropriate fora specific to understanding this risk and the approaches to managing this risk. It is encouraged that law enforcement representatives should be present within such discussions.*

1. INTRODUCTION AND METHODOLOGY

This chapter provides an overview of the scope of the study, before presenting the structure of the report and the adopted methodology.

1.1. Scope of the study

This study provides the LIBE Committee with an independent assessment of the existing legal frameworks for hacking by law enforcement, across the EU and globally. Primarily, this study focuses on the use of hacking techniques to gain remote access to an ICT system.

The key objectives of the study were to:

- Provide a **summary of the debates** held in international fora on hacking by law enforcement;
- Provide an **analysis of the legal basis for EU intervention** in the field of hacking by law enforcement;
- Provide a **comparison of the legal frameworks and practices** that relate to hacking by law enforcement in six EU Member States, with further comparative elements drawn from three non-EU countries; and
- Identify and **develop concrete policy proposals** based on the findings of the study.

1.2. Study methodology

The methodology used for this study comprises comparative and legal analysis techniques, in combination with expert opinion, to analyse the qualitative data collected through the following means:

- **Country reports** covering six Member States (France, Germany, Italy, the Netherlands, Poland, and the UK) and three non-EU countries (Australia, Israel and the USA) – see the rationales for the selection of countries, below;
- **Desk research** assessing information published at the EU level, internationally and in the case study countries;
- Extensive **interview** schedule covering European institutions, as well as national-level stakeholders in the case study countries. Although the study consulted law enforcement representatives, limited responses were received thereby limiting the input on law enforcement aspects of the study;
- **Expert workshop** with study experts Gerben Klein Baltink, Carly Nyst and Ivan Skorvánek.

The six case study countries, and the rationale for their selection, are presented in Table 1. Given the relatively new nature of this topic, the selection – conducted in consultation with the study experts – aimed to cover Member States considered to be more mature regarding both legal frameworks and public debate on hacking by law enforcement.

Table 1: Rationale for selected EU Member States

	France
	In 2011, the French Code of Criminal Procedure was amended to provide further interception powers to law enforcement authorities. Furthermore, Loi nº 2016-731 of 3 June 2016 provided law enforcement with the permission to remotely access computers and other devices.
	Germany
	Germany is renowned for its landmark Constitutional Court case that established a new basic right for the confidentiality and integrity of computer systems (Decision BvR 370/07). Germany also has legal provisions for hacking practices through the Code of Criminal Procedure and the Federal Criminal Police Act (*Bundeskriminalamtgesetz* – BKAG).
	Italy
	Law enforcement hacking practices have been in use in Italy for several years; in particular, the use of trojan horses. As such, Italy has experienced contrasting case-law decisions since 2009 and widely criticised legislative proposals. These developments paved the way for a new legislative bill, presented in February 2017, which approaches the legislation of hacking by law enforcement with a strong technical focus; an approach that differs from previous bills.
	Netherlands
	The Netherlands has experienced significant public debate on the topic of hacking by law enforcement in recent years. As such, the Computer Crime III Bill, a legislative proposal giving remote access powers to law enforcement, is making its way through the Dutch Parliament.
	Poland
	Several key developments have taken place in Poland related to hacking by law enforcement. Since the 2016 amendments to the Police Act, Polish law enforcement agencies now have the power of covert access to information systems. Furthermore, the Venice Commission, a Council of Europe (CoE) advisory body, published an extensive analysis of these provisions.
	United Kingdom
	Often the centre of debates on surveillance by law enforcement and the security and intelligence services, the UK has taken significant steps to legislate the security and intelligence services, as well as hacking by law enforcement. The Investigatory Powers Act, which came into effect in November 2016, provides the basis for these 'equipment interference' powers.

The three non-EU countries are **Australia, Israel and the US**. These three countries were selected in consultation with the study experts. The selection was based on a range of criteria, including the maturity of the legal framework, debate and practices, and geography.

1.3. Structure of the Report

The report is structured as follows:

Chapter 1. Sets out the scope of the study, the methodological approach and the structure of the report (this chapter);
Chapter 2. Provides a summary of the debates at international and EU fora on the use of hacking techniques by law enforcement agencies;
Chapter 3. Presents an analysis of the legal basis for EU intervention on this matter;
Chapter 4. Focuses on evaluating and comparing Member State legal frameworks and practices for hacking by law enforcement, based primarily on the EU country reports;
Chapter 5. Builds on the above chapters, outlining the conclusions of the study; and
Chapter 6. Based on the study findings, presents recommendations and concrete policy proposals for the consideration of the LIBE Committee.

In addition, the appendices to this report present: six EU country reports (Appendix 1); three non-EU country reports (Appendix 2); and a bibliography (Appendix 3).

2. SUMMARY OF INTERNATIONAL AND EU DEBATES

This chapter presents a summary of the **key international discussion points** related to the use of hacking practices by law enforcement agencies. It primarily centres around concerns raised and recommendations provided through UN and EU fora, although examples will be drawn from the national-level discussions, which in some cases represent a more mature debate.

The basis on which the international and EU-level debates summarised below are conducted is the increasing prevalence of **encryption technologies**. As such, section 2.1 will outline the debates related to encryption, including its increasing importance to society and its prominent role as an investigative barrier in the 'Going Dark' debate.

Within this backdrop, this chapter will present the debates on hacking by law enforcement. Firstly, the debates on the **benefits hacking techniques provide to law enforcement agencies** will be presented. Secondly, the discussions on the **risks posed by the use of hacking techniques by law enforcement agencies** will be summarised – it has been found that these risks comprise the vast majority of debates on the topic. More specifically, these risks relate to: the fundamental right to privacy; the security of the internet and, more generally, information communications technologies (ICTs); jurisdiction; and, to a lesser extent, the regulation of the sale of hacking tools.

Given the material scope of this study (established in section 1), it is worth noting that many of these debates, *in situ*, related to surveillance at the level of the security and intelligence services. However, the points raised are considered applicable, as a baseline, to the use of hacking practices by law enforcement agencies.

2.1. Encryption as an investigative barrier

Cryptography and, in particular, its applications in encryption, has been a recurring subject of discussion over recent decades, and provides important context for international debates on the use of hacking by law enforcement agencies. Since the seminal 1976 paper by Diffie and Hellman,[8] encryption – including the ability to securely communicate data over modern communications networks – has been widely available to citizens and businesses and not the sole preserve of governments. This widespread availability of encryption technologies led to the so-called 'Crypto Wars', which were characterised by the attempts of the US Government, through several policy measures, to develop the capabilities to decrypt all encrypted data.[9]

The first policy solution presented was the use of a 'key escrow' system. In such a system, a copy of each unique encryption key would be kept by the Government or a third party so that data could be decrypted using the appropriate key when necessary. However, the system faced much international criticism and, by 1997, there was an overwhelming body of evidence opposing all variants of the 'key escrow' system.[10]

Meanwhile, US export controls placed strict limits on the strength of the encryption technologies that could be exported from the USA. As a result, the spread and adoption of US-developed strong encryption tools was hindered and many US companies subsequently exported weaker encryption tools. However, around 2000, this policy stance weakened and export controls were relaxed in the face of significant criticism that the controls undermined

[8] Diffie, W. and Hellman, M. 1976. New Directions in Cryptography. *IEEE Transactions in On Information Theory*. Vol. IT-22, No. 6, November 1976.

[9] Open Technology Institute. 2015. Doomed to repeat history? Lessons from the Crypto Wars of the 1990s.

[10] Open Technology Institute. 2015. Doomed to repeat history? Lessons from the Crypto Wars of the 1990s.

US competitiveness and individual privacy, whilst resulting in the loss of billions of dollars of business.[11]

In turn, an **international consensus emerged supporting the development of strong encryption capabilities**. This consensus is evidenced by the 2015 report of the Special Rapporteur for the Human Rights Council,[12] which states the following:

> *"States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows"*

Furthermore, this consensus is supported by law enforcement representatives, such as the International Association of Chiefs of Police (IACP)[13] and, at the EU-level, Europol, who released a 2016 Joint Statement on the topic with ENISA.[14]

With this said, however, the **debate on encryption has intensified since 2015**, primarily at national-level. In particular, this is a result of the FBI v. Apple case[15] and the related debate surrounding the cooperation of vendors; the introduction of new legislation on the use of hacking techniques by law enforcement in the Netherlands, Poland and the UK;[16] and the increasing prominence of end-to-end encryption capabilities on emerging communications applications.[17]

Key figures in this debate – including (former UK Prime Minister) David Cameron and (current FBI Director) James Comey – have stated that bypassing encryption is often beyond the technical capabilities of law enforcement agencies, and therefore a threat to national security;[18] a statement supported by the law enforcement community. For example, high-ranking investigative personnel from the US, France, the UK and Spain collaborated to write an article for the *New York Times*.[19] Amongst other example, the article stated that, from October to June 2015, even with warrants, 74 iPhones could not be accessed by the Manhattan district attorney's investigators. As such, this article and other law enforcement representatives have inferred that the inability to access such data results in impunity.

This issue – i.e. the adverse impact of encryption capabilities and default encryption settings on the ability of law enforcement investigations to access data – is referred to as the 'Going Dark' phenomenon.[20]

Picking up where the 'Crypto Wars' left off, and primarily instigated under the threat of terrorism and cybercrime, the current debate therefore centres on how law enforcement and intelligence agencies may lawfully bypass encryption.

---

[11] Open Technology Institute. 2015. Doomed to repeat history? Lessons from the Crypto Wars of the 1990s.

[12] UN Human Rights Council. 2015. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/29/32.

[13] IACP Summit Report. 2015. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence.

[14] ENISA and Europol. 2016. On lawful criminal investigation that respects the 21st Century data protection. Europol and ENISA Joint Statement.

[15] Why is Apple objecting to the government's order? – Apple letter to customers http://www.apple.com/customer-letter/answers/; http://www.digitaltrends.com/mobile/apple-encryption-court-order-news/.

[16] See the Netherlands, Poland and UK country reports in Appendix 1.

[17] Ermoshina, K., Musiani, F. and Halpin, H. 2017. End-to-end Encrypted Messaging Protocols: An Overview. Accessed on 01.02.17 at: https://hal.inria.fr/hal-01426845/document.

[18] Abelson, H. et al. 2015. Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. *Computer Science and Artificial Intelligence Laboratory Technical Report.*

[19] Vance, C. Y., Molins, F., Leppard, A. and Zaragoza, J. 2015. When Phone Encryption Blocks Justice. The Opinion Pages. *The New York Times*, August 11, 2015.

[20] Comey, J. 2014. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? *FBI News*

International figures, such as David Cameron, James Comey and NSA Director Adm. Michael Rogers, have recently appealed for technology vendors to provide a 'backdoor' that allows the decryption of data for law enforcement and intelligence agencies.[21] This would involve vendors deliberately building vulnerabilities into their systems to facilitate the circumvention of encryption.[22] Furthermore, in a 2016 joint speech, the French and German Interior Ministers, Bernard Cazeneuve and Thomas de Maizière, recognised the importance of strong encryption to society whilst simultaneously insisting that the encrypted communications of targets must be available for law enforcement investigations and judicial proceedings, through cooperation with the vendors.[23] This potentially contradictory statement suggests that further debate on the subject is necessary at both the international and national levels.

However, computer scientists – as during the 'Crypto Wars' – are providing strong arguments against the above claims. Primarily, these stakeholders reiterate the risks to security, which remain the same as in previous decades, further stating that backdoor access would represent a "U-turn from the best practices now being deployed to make the Internet more secure".[24] Concerns have also been raised about jurisdictional access. For example, if a service provider sells its products in multiple countries, does it have to provide (identical or agency/nation-specific) backdoor access to all the relevant national governments – including those with questionable rule of law, democratic practices, and respect for human rights?

Some stakeholders have even placed doubt on the existence of a law enforcement challenge. The abovementioned report of the Human Rights Council, for example, states that "law enforcement and intelligence agencies assert" [25] this position, without supporting this view and the Centre for Democracy and Technology stated that the current 'golden age of surveillance' provides these agencies with more personal data than they could ever previously obtain.[26]

In addition to these concerns raised by specialists, the international and national-level debates have led to increasing public opinion against backdoor approaches, as highlighted by the abovementioned report of the Human Rights Council.[27] However, as repeatedly noted in the 2016 report of the Special Rapporteur on the right to privacy, in reference to the debates held in the UK's House of Lords, many individuals debating legislation on these matters, and encryption in particular, do not understand the topic.[28] More specifically, the Special Rapporteur states that "if the members of the House of Lords were to understand the

[21] David Cameron. 2015. PM: spy agencies need more powers to protect Britain, https://embed.theguardian.com/embed/video/uk-news/video/2015/jan/12/david-cameron-spy-agencies-britain-video.

[22] Timm, T. 2014. The government wants tech companies to give them a backdoor to your electronic life. *The Guardian*. https://www.theguardian.com/commentisfree/2014/oct/17/government-internet-backdoor-surveillance-fbi.

[23] Franco-German initiative on internal security in Europe. 2016. Speech by Bernard Cazeneuve, French Minister of the Interior, and Thomas de Maizière, Minister of the Interior of the Federal Republic of Germany on 23 August 2016, Paris. Accessed on 01.02.17 at: http://www.interieur.gouv.fr/Archives/Archives-ministre-de-l-interieur/Archives-Bernard-Cazeneuve-avril-2014-decembre-2016/Interventions-du-ministre/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe.

[24] Abelson, H. et al. 2015. Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. *Computer Science and Artificial Intelligence Laboratory Technical Report.* p.2.

[25] UN Human Rights Council. 2015. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/29/32.

[26] Centre for Democracy and Technology. 2011. 'Going Dark' Versus a 'Golden Age for Surveillance'.

[27] Abelson, H. et al. 2015. Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. *Computer Science and Artificial Intelligence Laboratory Technical Report.*

[28] UN General Assembly. 2016. Right to privacy report of the Special Rapporteur on the right to privacy. A/71/368. Paragraphs 28-32.

arguments presented […] they would then understand why attempts to legislate weakened encryption into being are a bad idea and particularly daft in practice".[29]

With this said, one alternative to 'backdoors' is the use of hacking techniques by law enforcement agencies. For instance, these hacking techniques may allow law enforcement agencies to access data before it is encrypted (i.e. at the source) or access passwords used to encrypt data.

Law enforcement representatives, such as the IACP and Europol, state that the use of hacking techniques as an investigative tool brings significant improvements in investigative effectiveness. In fact, the IACP state that law enforcement agencies are not able to investigate illegal activity and prosecute criminals effectively without evidence collected using hacking techniques.[30] Although the use of hacking techniques will bring improvements in investigative effectiveness, the significant amount and sensitivity of data that can be accessed through these means acts as a stimulus for another key debate: **ensuring the protection of the fundamental right to privacy**.

Furthermore, the use of hacking techniques by law enforcement is not the only solution to 'Going Dark', nor the only alternative to 'backdoor' approaches. Other possibilities include requiring users to provide their password or decrypt their data; and requiring technology vendors or service providers to bypass the security of their own products and services. These alternatives are out of scope for this study and will not be discussed.

2.2. Fundamental rights considerations

As stipulated in the Charter of Fundamental Rights of the European Union (Article 7) and the European Convention on Human Rights (Article 8), the right to privacy is a qualified right, meaning that it can be lawfully restricted under certain, specified circumstances. This is also relevant to Article 11 on the right to freedom of expression and information. A restriction of these rights must be:[31]

- In accordance with law;
- Necessary and proportionate; and
- For one or more of the following legitimate aims:
  - the interests of national security;
  - the interests of public safety or the economic well-being of the country;
  - the prevention of disorder or crime;
  - the protection of health or morals; or
  - the protection of the rights and freedoms of others.

This is not a new concept. Coercive law enforcement activities have restricted the right to privacy based on appropriate legal provisions for hundreds of years (e.g. the Fourth Amendment of the US Constitution, as passed in 1789[32]). However, it is widely recognised that law enforcement hacking has the potential for increased invasiveness when compared with traditional coercive activities (e.g. wiretapping, house searches etc.). For instance, in many cases, the use of hacking tools can provide law enforcement with access to all data held on a device, as well as all information flows in and out of the device; this is likely to

[29] UN General Assembly. 2016. Right to privacy report of the Special Rapporteur on the right to privacy. A/71/368. Paragraphs 28-32.

[30] IACP Summit Report. 2015. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence.

[31] Liberty Human Rights. Article 8 Right to a private and family life. Accessed on 06.01.17 at: https://www.liberty-human-rights.org.uk/human-rights/what-are-human-rights/human-rights-act/article-8-right-private-and-family-life.

[32] Friedman, B. and Kerr, O. Common Interpretation: The Fourth Amendment IV. Accessed on 15.03.17 at: https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv.

constitute the collection of a much greater amount of data, as well as the collection of much more sensitive data. In early 2017, this was illustrated by Dutch police, who accessed and decrypted, using commercially available tools, seven terabytes (TB) of data stored on a server belonging to Dutch firm Ennetcom.[33] To put this into perspective, it is estimated that only one TB can hold approximately 86 million pages of Microsoft Word documents or 310,000 photos.[34]

As such, as long as the hacking practices are necessary to overcome the 'Going Dark' problem and proportionate to fulfilling this aim, national-level legal frameworks may restrict the right to privacy through the legal stipulation of appropriate limitations and safeguards considering the above points. This section presents the discussions held in international fora on the issues related to limiting the right to privacy through hacking practices, including the appropriate legal safeguards.

Before the discussions on the appropriate limitations and safeguards are summarised, however, it should be noted that the debates at **international and EU fora do not question the general necessity and proportionality of law enforcement hacking as practices** to overcome the reported challenges faced by law enforcement agencies; i.e. the discussions presume such necessity and proportionality and focus on how national-level legislation should govern such invasive activities and the restrictions they place on privacy.

In November 2016, the UN General Assembly adopted its **third resolution on the right to privacy in the digital age**.[35] Reaffirming the 2013[36] and 2014[37] resolutions on the same topic, the General Assembly expressed its concern regarding the threats posed to human rights by State-driven surveillance, interception of digital communications and data collection capabilities.[38] Specifically, this concern relates to the "interlinked and mutually dependent"[39] rights to privacy and freedom of opinion and expression, as enshrined internationally in Articles 12 and 19 of the Universal Declaration of Human Rights (UDHR)[40] and Articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR).[41] Both documents stipulate that "everyone has the right to the protection of the law against such interference or attacks".[42]

In addition to highlighting the UN's concerns, these resolutions offer a range of recommendations for UN States to consider (see Box 1).

[33] Paganini, P. 2017. Ennetcom – Dutch Police confirmed to have decrypted BlackBerry PGP messages in a criminal case. Article on Security Affairs, 10 March 2017.

[34] Brown, K. 2014. A Terabyte of Storage Space: How Much is Too Much? University of Oregon blog: The Information Umbrella: Musings on Applied Information Management.

[35] UN General Assembly. 2016. The right to privacy in the digital age. A/C.3/71/L.39/Rev.1.

[36] UN General Assembly resolution 68/167 of 18 December 2013 on the right to privacy in the digital age.

[37] UN General Assembly resolution 69/166 of 18 December 2014 on the right to privacy in the digital age.

[38] UN General Assembly. 2016. The right to privacy in the digital age. A/C.3/71/L.39/Rev.1.

[39] UN General Assembly. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40.

[40] UN. 1948. Universal Declaration of Human Rights. Article 12.

[41] UN General Assembly. 1966. International Covenant on Civil and Political Rights, Treaty Series, vol. 999, p.171, Article 17.

[42] *Id.,* Article 17(2).

Box 1: Key recommendations from the UN General Assembly's 2016 resolution on the right to privacy in the digital age.

Key recommendations of the third UN General Assembly resolution on the right to privacy in the digital age (2016).

- Review "procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data"[43] – this recommendation is also encouraged by the World Summit on the Information Society[44];
- Establish and maintain existing oversight mechanisms capable of ensuring transparency and accountability – these should be "independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic"[45] mechanisms; and
- Provide an effective remedy for the subjects of unlawful or arbitrary surveillance[46].

Furthermore, the third resolution recognises the need to further discuss and analyse the promotion and protection of the right to privacy in the digital age, covering "procedural safeguards, effective domestic oversight and remedies […] as well as the need to examine the principles of non-arbitrariness and lawfulness, and the relevance of necessity and proportionality assessments".[47] Thus, the resolution also commits to the continued consideration of the issue.[48]

Beyond these General Assembly resolutions, the international-level debates have primarily evolved through the work of the Human Rights Council,[49] the Special Rapporteur on the right to privacy[50] and the Special Rapporteur on the right to freedom of opinion and expression.[51] By contrast, international justice sector bodies – e.g. the UN Office on Drugs and Crime (UNODC), the International Criminal Police Organisation (Interpol) and the Commission for Crime Prevention and Criminal Justice (CCPCJ) – have published very little on the topic.

Primarily, the documentation published by these entities echoes, while adding depth and detail to, the third resolution. A 2014 report by the UN High Commissioner for Human Rights[52] notes that **many UN contributors consider surveillance, interception and the collection of personal data to be necessary and effective law enforcement practices**, when used **in compliance with an appropriate legislative framework**. This statement is complemented by the 2013 *Report of the Special Rapporteur on the right to freedom of opinion and expression,*[53] which provides the following legislative recommendations that are applicable to the case of hacking by law enforcement:

- Complete **transparency in the use and scope** of surveillance techniques and powers;
- **Independent supervision and oversight** mechanisms capable of ensuring transparency and accountability;

[43] UN General Assembly. 2016. The right to privacy in the digital age. A/C.3/71/L.39/Rev.1, point 5(c), p.5.

[44] UN General Assembly. 2016. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. A/RES/70/125. Paragraphs 44 & 46.

[45] UN General Assembly. 2016. The right to privacy in the digital age. A/C.3/71/L.39/Rev.1, point 5(d), p. 5.

[46] *Id*., point 5(e), p. 5.

[47] UN General Assembly. 2016. The right to privacy in the digital age. A/C.3/71/L.39/Rev.1, pp. 2-3.

[48] *Id*., point 10, p. 6.

[49] Human Rights Council resolutions 28/16 of 26 March 2015 and 32/13 of 1 July 2016; and A/HRC/27/37.

[50] A/HRC/31/64 and A/71/368.

[51] A/71/373, A/HRC/23/40 and A/HRC/29/32.

[52] UN High Commissioner for Human Rights. 2014. The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/27/37.

[53] UN Human Rights Council. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40.

- **Safeguards relating to the nature, scope and duration of possible measures**, as well as the grounds for ordering them and the remedy provided by national law; and
- **Notification of individuals** that have been subjected to communications surveillance.

This report also reiterates the need for clarity and precision in the legal framework and the importance of the principles of necessity and proportionality.

Furthermore, the UN High Commissioner's report further adds to this picture, stating the case that many UN States currently have "[in]adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight",[54] which contribute to an overall lack of accountability for interference in the right to privacy. This position is further supported by the 2016 *Report of the Special Rapporteur on the right to freedom of opinion and expression,*[55] which states that relevant legislation in this field is often too broad and does not sufficiently engage the public.

Despite the extensive legal recommendations that aim to qualify these interference practices and human rights, recent ECHR jurisprudence[56] suggests that governments are still not appropriately amending their legal frameworks and practices.

Box 2: National-level debates on fundamental rights.

National-level debates.

At the national level, the debate around the protection and promotion of human rights has become increasingly entrenched at the law–technology nexus. In particular, the debate surrounds the lack of specificity appropriated to the use of zero-day exploits, malware, botnet mitigation techniques and other technical means in national-level legislation. For instance, criticism has been levied at certain national laws, such as those in the UK, the US and Australia, for allowing the use of advanced technical means for non-targeted hacking in which an unspecified number of devices can be investigated and innocent users may be impacted. According to some civil society organisations, these practices do not appropriately represent the principle of proportionality and negatively impact judicial oversight.[57,58]

Furthermore, civil liberties groups argue that the use of "malware and zero-day exploits is more invasive than other forms of permissible searches [such as those primarily discussed in UN fora] because the consequences and collateral damage associated with their use are inherently unpredictable and often irreversible".[59] This argument states that the increased invasiveness of these hacking practices means that they cannot be governed appropriately by national laws relating to the interception of communications or other 'analogous' comparators – as is the case for the remote access warrant procedures outlined in Rule 41 of US legislation – as they do not fall within the bracket of 'reasonable necessity'.[60]

As discussed above, these technical means are reported to be available to national-level law enforcement agencies and the discussion primarily relates to how their use can be reconciled with the protection of human rights. Parallels can be drawn with the International

[54] *Id.,* paragraph 47.

[55] UN General Assembly. 2016. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/71/373.

[56] See, e.g., ECHR cases of Szabo v. Hungary, Zakharov v. Russia.

[57] Liberty Group. 2015. Liberty's response to the Home Office consultation on the Equipment Interference Code of Practice.

[58] Kim, S. 2016. Whose World Is This?: US and UK Government Hacking.

[59] ACLU, Second Comment, supra note 54, p. 18.

[60] Thompson, R.M. 2016. Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Congressional Research Service.

Telecommunication Union's conclusion on the technical aspects of lawful interception that, whilst important, "accurate international standards-based network forensics technologies for lawful interception, data retention and network management are needed to meet national requirements".[61]

2.3. Security of the internet and ICTs

The technological advances mentioned above have made encryption, if implemented correctly, extremely difficult, if not impossible, to 'break'. However, as the cybersecurity field knows only too well, there are always system vulnerabilities waiting to be exploited. These vulnerabilities are what hackers use and now law enforcement agencies are reported to be increasingly using these methods for circumventing the security of ICTs in place of attempts to 'break' encryption. For example, German law enforcement has the legal possibility to inject police malware into a device to intercept communications data at source before they are encrypted for transit.[62]

In particular, although not exclusively, academics report that governments are increasingly reliant on zero-day exploits,[63] which, like all vulnerabilities, are potentially detrimental to the security of the internet. Furthermore, these vulnerabilities represent a conflict of interests for law enforcement agencies. Reporting knowledge of vulnerabilities to the vendors allows them to be fixed; however, retaining knowledge of vulnerabilities allows law enforcement to use that vulnerability to access data again and again until its discovery.

A specific point of interest is the way in which specific third parties acquire and sell sofar unknown zero-day exploits to law enforcement agencies. It is unclear in what way the trade in these zero-day exploits is under any form of oversight or control by governments. As this has not been discussed in international fora, the discussion below presents the most mature national-level debates on the topic.

A zero-day exploit uses a vulnerability that is "discovered and exploited prior to public awareness or disclosure to the vendor".[64] The nature of these unknown vulnerabilities present many significant risks to information security, including:

i. they may exist in any software or hardware;[65]
ii. attacks that exploit zero-day vulnerabilities are often not discovered organically for months or even years – according to cybersecurity company FireEye, the average day of discovery is 310 days and the average attack lasts eight months;[66] and
iii. zero-day threats are not easily detected as most traditional security tools rely on known, confirmed threats.[67]

These risks characterise an environment in which significant harm can be caused. A notable example is "Operation Russian Doll", where zero-day vulnerabilities in Adobe Flash and Windows were exploited to mount a malicious attack on an unnamed US government entity.[68]

---

[61] International Telecommunication Union (2008) Technical Aspects of Lawful Interception. ITU-T Technology Watch Report 6.

[62] See Appendix 1: Germany Country Report for more information.

[63] Bellovin, S.M., Blaze, M., Clark, S. and Landau, S., 2014. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. Nw. J. Tech. & Intell. Prop., 12, p. i.

[64] *Id.,* p. 20.

[65] FireEye. 2017. What is a Zer-Day Exploit? Accessed on 15.03.17 at: https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html.

[66] FireEye. 2015. Zero-Day Danger: A Survey of Zero-Day Attacks and What They Say About the Traditional Security Model. White Paper.

[67] *Id.*

[68] FireEye. 2015. Zero-Day Danger: A Survey of Zero-Day Attacks and What They Say About the Traditional Security Model. White Paper.

Debates around hacking by law enforcement and the security of the internet have therefore focused heavily on zero-day exploits due to the abovementioned risks, and because there is little knowledge or guidance regarding their use in national-level legislation.[69] The American Civil Liberties Union (ACLU), for instance, argues that the US Government should report, rather than exploit, zero-day vulnerabilities, and is putting individuals at risk by not doing so.[70] Furthermore, the President's NSA Group stated that "in almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities – 'patching' them – strengthens the security of US Government, critical infrastructure, and other computer systems."[71]

However, some academics counter this argument, stating that using zero-day exploits is necessary and "preferable",[72] and also suggest policies by which any potential damage could be limited.[73] These policies include: the implementation of technical defences to prevent rediscovery of the vulnerability; the requirement for law enforcement agencies to report the vulnerability when it is discovered and to gain a warrant to continue (barring emergency circumstances); the deletion (or ignoring) of any additional information discovered not specified in the warrant; and the regulation of exploitation tools under 'dual-use' restrictions.[74]

As mentioned above, however, there has been a limited policy response from national level authorities. One example is the Vulnerability Equities Process (VEP) being implemented in the US.[75] The VEP requires an interagency Equities Review Board to making decisions on whether to retain a vulnerability for government use or disclose it to the appropriate vendor for patching.[76] Although much of the detail is classified, White House Cybersecurity Coordinator Michael Daniel has stated that the existing VEP uses a "deliberate process that is biased toward responsibly disclosing vulnerabilit[ies]".[77] Whilst groups have highlighted concerns around the effectiveness of the process,[78] it is encouraging to see a policy response that attempts to responsibly govern the use of zero-day exploits.

As will be discussed in more detail in section 4.4, the only EU Member State examined with a response to zero-day vulnerabilities is the Netherlands. The Dutch Computer Crime III Bill permits the use of zero-day vulnerabilities while dictating that law enforcement must not purchase zero-day vulnerabilities and must report any exploited vulnerabilities. As for the US, recognition of this challenge is a positive factor; however, civil society actors have

---

[69] See section 4.4 Technical Means Used by Law Enforcement.

[70] ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches Of Electronic Storage Media (2016).

[71] Review Grp. on Intelligence and Commc'n Techs., Liberty and Security in a Changing World 187 (2013), p. 220, cited *Id*.

[72] Bellovin, S.M., Blaze, M., Clark, S. and Landau, S., 2014. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. Nw. J. Tech. & Intell. Prop., 12, p. i. p. 64.

[73] Bellovin, S.M., Blaze, M., Clark, S. and Landau, S., 2014. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. Nw. J. Tech. & Intell. Prop., 12, p. i.

[74] *Id.*

[75] Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process (2010). Found at https://www.eff.org/files/2016/01/18/37-3_vep_2016.pdf.

[76] Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process (2010). Found at https://www.eff.org/files/2016/01/18/37-3_vep_2016.pdf. p. 3.

[77] Daniel, M (2014), "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities", White House Blog, ("Daniel Blog Post"), https://www.whitehouse.gov/blog/2014/04/28/heart-bleed-understanding-when-we-disclose-cyber-vulnerabilities.

[78] Schwartz, A. and Knake, R. (2016). Government's Role in Vulnerability Disclosure. The Cyber Security Project

criticised the application of these legal provisions, reporting that Dutch law enforcement procure off-the-shelf tools that exploit both known and unknown vulnerabilities.[79]

Although recognition of this challenge and mature debate has begun in a few countries, the lack of discussion on these points at international and EU fora should be rectified considering the potential impacts of the use of zero-day vulnerabilities and other hacking methods on the security of the internet and ICTs.

2.4. Jurisdictional challenges

As touched on above, jurisdiction is another area of focus regarding debates on the use of hacking techniques by law enforcement agencies. Although not discussed at length at the EU or international level, a 2010 Council of Europe discussion paper,[80] in addition to academic research,[81] provides important insight into this area of challenge.

Furthermore, Article 18 (Production Order) of the Convention on Cybercrime of the Council of Europe (Budapest Convention) requires parties to adopt a set of procedural powers to secure electronic evidence, such as search and seizure of computer systems, production orders for data, interception of communications etc. Under this article, service providers are required to produce any "specified" computer data requested by Law Enforcement Authorities. In practice, in the EU, cooperation between LEAs and service providers vary. The table below provides practical examples of cooperation between some of the major service providers and LEAs. It also illustrates the type of data that service providers are willing to disclose to LEAs.

According to practitioners, service providers execute requests from law enforcement or even judicial authorities in a variety of ways. This diversity seems to greatly affect investigating authorities when examining all the criteria to exert jurisdiction.[82]

Table 2: Current practices of cooperation between LEAs and service providers[83]

Apple
Apple will accept service of legally valid law enforcement information requests by email from law enforcement agencies, provided these are transmitted from the official email address of the law enforcement agency concerned. Unless emergency procedures are used, Apple only discloses content upon a search warrants pursuant to an MLA request or a similar cooperative effort.
Facebook
Requests from regions other than the USA or Canada need to be sent to Facebook Ireland and are handled by the Facebook Ireland law enforcement unit.
Google
For requests from outside US, Google can provide the same type of data as the one provided for request inside US if the request passes through an MLA process.

[79] See Appendix 1: Netherlands Country Report for more detail.

[80] Council of Europe. 2010. Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Discussion paper, p. 5.

[81] Koops, BJ & Goodwin, MEA. 2014. *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, available at https://ssrn.com/abstract=2698263.

[82] Eurojust, Strategic seminar "Keys to Cyberspace", 2 June 2016, Outcome report.

[83] CoE, Octopus Conference – The Voluntary Cooperation Model and Production Orders for Subscriber Information.

Microsoft

For requests from outside the US, Microsoft can provide basic subscriber information (BSI) and transactional data, directly to upon receipt of a request to their office in the Republic of Ireland. For content data, an MLA request needed.

However, the Budapest Convention is based on the assumption that the physical location of the data is known[84]. Given the nature of the internet, the expansion of cloud computing services and the fact that these services and channels are owned and controlled by private international companies, many services are provided across borders. Therefore, law enforcement agencies may not know in which country, or even continent, certain data reside – this has resulted in the concept of "loss of location",[85] as termed in the Council of Europe paper, or more precisely, "**loss of knowledge of location"**.[86] In fact, in the case of cloud computing, even the service provider might not know where such data are located.[87]

Linked to this challenge is the risk that, without precise detail of the location of such data, law enforcement agencies may remotely access data located in the jurisdiction of another country, thereby breaching the "international legal principle of territorial sovereignty which sets forth that no state may enforce its jurisdiction within the territory of another sovereign state".[88] Additionally, such use of hacking techniques may also introduce the associated risks of such access, as discussed above, in the systems of other countries.

The traditional law enforcement response to such instances would be to seek cooperation with the other country through procedures for mutual legal assistance, as governed by the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the EU, which uses as its basis the European Convention on Mutual Assistance in Criminal Matters (CoE, 12.06.1959). However, mutual assistance procedures are deemed to be "cumbersome or ineffective".[89] Given the ease with which such data can be moved with high frequency, alongside the difficulties identifying the location of such data, this assessment of mutual assistance is particularly true when law enforcement agencies are seeking digital evidence.[90]

Moreover, in some instances, law enforcement agencies may not even know they are breaching jurisdictional boundaries. Hence, the debate has revolved around example cases where law enforcement agencies have used hacking techniques to access data beyond their jurisdiction. Two such examples are presented in Box 3.

---

[84] Eurojust, Strategic seminar "Keys to Cyberspace", 2 June 2016, Outcome report.

[85] Council of Europe. 2010. Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Discussion paper, p. 5.

[86] Koops, BJ & Goodwin, MEA. 2014. *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, available at https://ssrn.com/abstract=2698263, p. 42.

[87] Council of Europe. 2010. Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Discussion paper, p.5.; see also Koops, BJ & Goodwin, MEA. 2014. *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, available at https://ssrn.com/abstract=2698263.

[88] Council of Europe. 2010. Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Discussion paper, p.5.; see also Stein/von Buttlar, Völkerrecht, Cologne, 11th ed. 2005, pp. 186–196; Ipsen, Knut, Völkerrecht, Munich, 5th ed. 2004, pp. 310–318.

[89] Koops, BJ & Goodwin, MEA. 2014. *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, available at https://ssrn.com/abstract=2698263.

[90] *Id.,* p. 7.

Box 3: Examples of the use of hacking by law enforcement in the US and the jurisdictional challenges.

US authorities (2015) – the FBI received intelligence from an unspecified foreign law enforcement agency that a US-based IP address was associated with a website, hosted as a Tor hidden service (i.e. not on the 'open' internet), that was known to be distributing child pornography.

As such, a magistrate judge granted a warrant to identify visitors to this site and the FBI ran a 'watering hole' attack which used a network investigative technique (NIT) to hack over 1,000 computers that visited the site over a 13-day period. Several criticisms have been levied at this investigation since a minimally redacted version of the warrant and supporting documentation was released as a legal exhibit – one key challenge was jurisdictional.

The NIT was not limited geographically – any visitor to the target website, irrespective of their location, was hacked. As a result, it has been reported that the NIT impacted the privacy and anonymity of persons in Denmark, Greece and Chile – countries outside the jurisdiction of the issued warrant. In fact, Federal Courts in Virginia and Oklahoma found that the use of an NIT "outside the geographic bounds of the issuing judge's district was invalid".[91]

Australian authorities (2016) – a further example of government hacking overseas was reported in 2016, when the Australian authorities allegedly used phishing attacks to bypass Tor software as part of a child pornography investigation and, in doing so, remotely hacked a computer in Michigan.[92] Although the FBI retrieved the information from the Australian authorities as it concerned an American citizen, whether and how the Australian agencies gained an overseas warrant was disputed.[93] Examples such as this have led to much debate about the need for more transparency in gaining international hacking warrants.[94]

Furthermore, although some national legislation, such as the Investigatory Powers Act in the UK[95] and the Dutch Computer Crime III Bill,[96] permits the use of hacking beyond national jurisdictions in certain circumstances, the nature of anonymising technology means that it is very difficult for law enforcement and intelligence agencies to give prior warning or gain consent from international governments until after the hacking has been conducted and the location of the target has been revealed.[97] Similarly, the Investigatory Powers Act only permits the use of equipment interference overseas by intelligence agencies[98] but, if the location is unknown, there is a chance that law enforcement agencies may also use such techniques on a foreign computer.

Although the above interpretation of territoriality in relation to international law is the dominant view, civil society and academic stakeholders have argued that the related debates at international and EU fora need to mature and discuss this topic in greater detail. Privacy International, for instance, although referring to cross-border surveillance activities more generally, "demand a set of recommendations to govern"[99] such practices. Moreover, a 2014

[91] Volz, D. 2015. FBI would gain new hacking power if search warrant rules change.

[92] Cox, J. 2016. Australian Authorities Hacked Computers in the US. Motherboard.

[93] Cox, J. 2016. Australian Authorities Hacked Computers in the US. Motherboard.

[94] Privacy International and Open Rights Group's Submission In Response To The Consultation On The Draft Equipment Interference Code Of Practice (2015).

[95] Investigatory Powers Act 2016 (c. 25) Part 6 – Bulk warrants Chapter 3 – Bulk equipment interference warrants

[96] Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III).

[97] Kim, S. 2016. Whose World Is This?: US and UK Government Hacking.

[98] Investigatory Powers Act 2016 (c. 25) Part 5 — Equipment interference.

[99] Kim, S. 2016. Whose World Is This?: US and UK Government Hacking.

report by Koops and Goodwin concludes that international law currently presents "considerably larger limits than possibilities for cross-border"[100] investigations related to the collection of digital evidence. As a first port of call, this report points to possibilities within Article 32(b) of the Cybercrime Convention but primarily calls for a fundamental rethink of the issue and the international approach to its resolution.[101]

Some initiatives have been launched to address jurisdictional challenges. The "Keys to Cyberspace" strategic seminar for instance was organised to assess the state of play in the US and the EU with regards challenges to establishing jurisdiction in the Cloud as well as discuss possible ways forward. Amendments to the Budapest Convention or an improvement of the situation within the EU would be welcome in order to ensure cooperation of service providers and set out minimum requirements and standards for requests for information form LEAs. However, these would only address a small part of the problem. It is widely recognised that a global solution needs to be found, although the sharing of best practices does already help. These include draft guide to help draft requests, creating specialised points of contact, or, going further, harmonising procedure for requests. [102]

2.5. Regulation of hacking tools

Since the release of detailed information on Gamma Group's spyware suite, *FinFisher*,[103] and the practices of Italian firm *Hacking Team*,[104] hacking tools have been extensively discussed at the international and EU levels.

In particular, such companies have been criticised in relation to the supply of hacking tools to nations whose specific intent was "violating human rights by means of censorship, mass surveillance, jamming, interception and monitoring"[105] (see Figure 1, p.16, for a list of countries supplied with *FinFisher* spyware). Therefore, civil society organisations have **questioned the current dual-use export control regimes and called for these companies to be properly regulated**.[106] The developments with regard to these regimes at the international and EU levels will be detailed below.

At the **international level**, dual-use exports are primarily regulated by the non-binding Wassenaar Arrangement, to which all EU Member States bar Cyprus are party. These revelations and associated criticisms led to amendments to Wassenaar in 2012 and 2013. These amendments expanded its coverage to include technology under the following terms: 'intrusion software', 'mobile interception or jamming equipment' and 'Internet Protocol (IP) network surveillance systems'.[107]

---

[100] Koops, BJ & Goodwin, MEA. 2014. *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, available at https://ssrn.com/abstract=2698263.

[101] *Id.,* pp. 12-13.

[102] Eurojust, Strategic seminar "Keys to Cyberspace", 2 June 2016, Outcome report.

[103] Marczak, B. et al. 2015. Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. Munk School of Global Affairs.

[104] Reporters without Borders. 2012. The Enemies of Internet, Special Edition: Surveillance. Accessed on 06.01.17 at: http://surveillance.rsf.org/en/hacking-team/.

[105] Immenkamp, B (European Parliamentary Research Service). 2017. Review of dual-use export controls: European Parliament Briefing: EU Legislation in Progress. Accessed on 10.03.17 at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf.

[106] Marczak, B. et al. 2015. Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. Munk School of Global Affairs.

[107] Bauer, S. and Bromley, M. 2016. The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World. Non-Proliferation Papers by the EU Non-Proliferation Consortium. No. 48.

Supporting guidance on the Wassenaar Arrangement further states that export licences should not be issued to a private company if their product may "be used for the violation or suppression of human rights and fundamental freedoms".[108]

At the **EU level**, dual-use exports are governed by the legally binding Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (Regulation 428/2009). Subsequent to Wassenaar, the EU's dual-use control list was amended in 2014 to include the abovementioned items. Furthermore, a Surveillance Technology Expert Group (STEG) was established by the EU's Dual-Use Coordination Group (DUCG) to examine the issue of regulating hacking tools and other surveillance technologies.[109]

However, even with these amendments, fundamental rights experts argue that these export control regimes do not prevent the exportation of hacking tools to the abovementioned governments.[110] The fact that the Wassenaar Arrangement is not legally binding, in addition to the "divergent interpretations and applications"[111] of the regime terminology at national level, are key drivers of this argument. Although Regulation 428/2009 is binding, it faces the same challenges with regard to Member State implementation as illustrated by the comprehensive Information Note published in the Official Journal of the 13 February 2015.[112] Furthermore, these experts state that, as the provisions related to hacking tools are modelled on the *FinFisher* spyware, the Wassenaar Arrangement and Regulation 428/2009 do not provide effective coverage of the diverse range of hacking tools that are available.[113] As such, there is a call for prohibition of the exportation of hacking tools to governments with low consideration for human rights.[114]

In line with these debates, the European Parliament has issued several resolutions since 2014[115] and the European Commission is conducting a review of the EU's export control policy, in line with Article 25(2) of Regulation 428/2009. The result of these activities is a **proposal, adopted by the European Commission on 28 September 2016, for the modernisation of the EU export control system**.[116]

A key aspect of the modernisation proposal is the introduction of the concept of 'human security', which aims to prevent the human rights violations associated with hacking tools, and other surveillance technologies, as described above – see Article 2(1)(b).[117] The objective

---

[108] The Wassenaar Arrangement – On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, About Us. http://www.wassenaar.org/.

[109] Bauer, S. and Bromley, M. 2016. The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World. Non-Proliferation Papers by the EU Non-Proliferation Consortium. No. 48.

[110] Nyst, C. 2017. Expert interview conducted for this study.

[111] Immenkamp, B (European Parliamentary Research Service). 2017. Review of dual-use export controls: European Parliament Briefing: EU Legislation in Progress. Accessed on 10.03.17 at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf.

[112] Information Note. Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items: Information on measures adopted by Member State in conformity with Articles 5, 6, 8, 9, 10, 17 and 22. (2015/C 51/08, p.8).

[113] Nyst, C. 2017. Expert interview conducted for this study.

[114] *Id.*

[115] Relevant European Parliament actions include: the European Parliament, Council and Commission joint statement on the review of the dual-use export control regime (2014); the European Parliament resolution of 17 December 2015 on arms export; the European Parliament resolution of 8 September 2015 on human rights and technology; the European Parliament resolution of 21 May 2015 on the impact of developments in European defence markets on security and defence capabilities in Europe; and the European Parliament resolution of 5 February 2014 on the ratification of the Arms Trade Treaty.

[116] Immenkamp, B (European Parliamentary Research Service). 2017. Review of dual-use export controls: European Parliament Briefing: EU Legislation in Progress. Accessed on 10.03.17 at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf.

[117] *Id.*

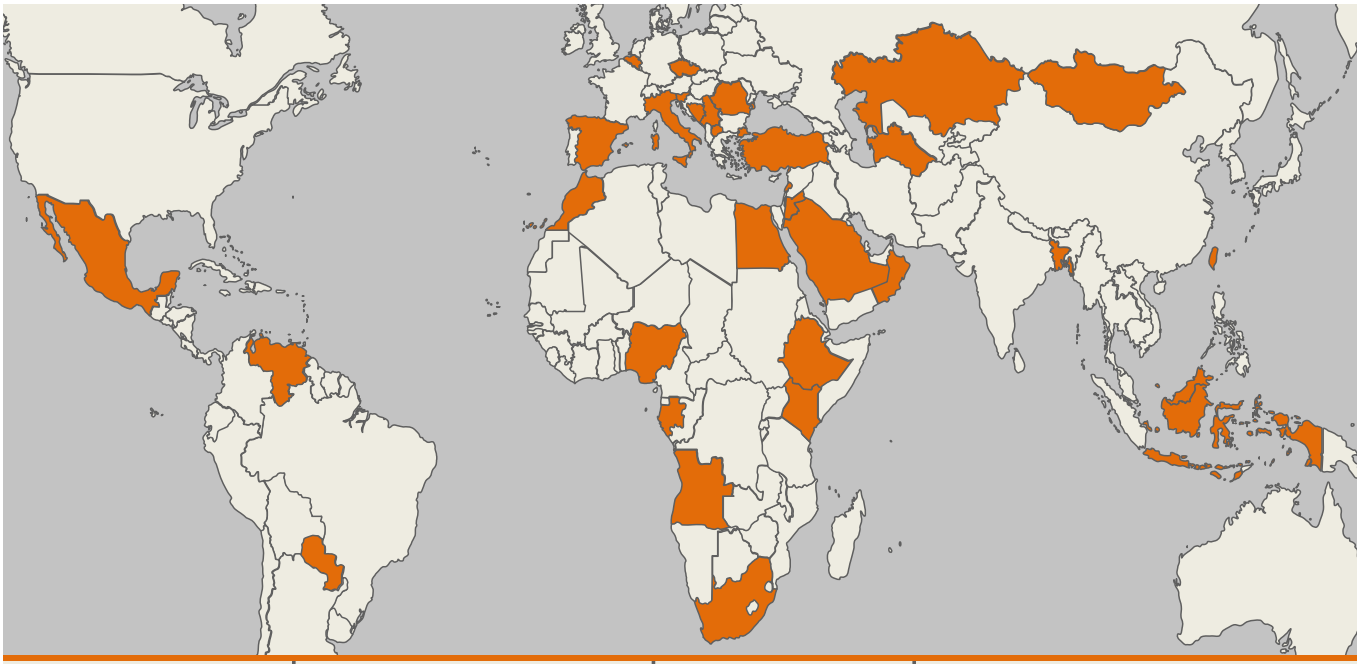
is to achieve this through the control of the three abovementioned types of technology, in addition to two new types – 'monitoring centres and data retention systems' – and the inclusion of a catch-all provision that would make it "obligatory to obtain an authorisation for the export of dual-use items not included in the control list destined for use by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law"[118] – Article 4(1)(e).

In addition to ensuring an increased focus on the human rights risks posed by the export of hacking tools, these provisions may lead to a shift beyond the civilian–military paradigm that has traditionally framed dual-use export controls to a system that covers the use of these technologies by law enforcement and intelligence agencies.[119]

Furthermore, the proposed provisions may assuage the criticisms of many in the cybersecurity community. These stakeholders argue that dual-use controls currently prevent legitimate activities related to the use of hacking tools[120]; the Commission's proposal, focusing on whether these tools will be used for violations of fundamental rights, may ease the burden for the export of legitimate hacking tools.

However, the concerns related to the Wassenaar Arrangement persist.

Figure 1: Countries to which FinFisher has been sold.[121]



Source: Optimity Advisors, adapted from Marczak et al. 2015.

[118] Immenkamp, B (European Parliamentary Research Service). 2017. Review of dual-use export controls: European Parliament Briefing: EU Legislation in Progress. Accessed on 10.03.17 at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf.

[119] Bauer, S. and Bromley, M. 2016. The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World. Non-Proliferation Papers by the EU Non-Proliferation Consortium. No. 48.

[120] Barth, B (2016). Executive branch concedes Wassenaar Arrangement must be renegotiated, not revised. *SC Media.*

[121] Marczak et al. 2015.Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation

In **conclusion**, the debates held in international fora primarily relate to the balance between the promotion and protection of human rights and the ability of law enforcement and intelligence agencies to access the data they require through surveillance, interception and collection of personal data – one aspect of which is the hacking practices employed by law enforcement agencies. These debates raise concerns over current legal frameworks and practices and provide recommendations for the rectification of the *status quo*. Further UN debates have covered the challenges faced by encryption and firmly stated the position of the UN in support of banning encryption backdoors, 'key escrow' or weakened encryption standards.

Additional debates related to the impacts of hacking by law enforcement agencies on the security of the internet and ICTs, the jurisdictional challenges related to hacking by law enforcement, and the regulation of hacking tools through the Wassenaar Arrangement have been almost solely conducted at national level and require maturing at the UN level.

3. EU LEGAL BASIS ANALYSIS

This chapter presents an analysis of the EU's competences to act in the field of hacking by law enforcement, discussing the potential legal bases for EU intervention.

The legal basis for the EU to adopt legislation concerning the use of hacking techniques by law enforcement in criminal investigations could potentially be based on:

- Shared competence in the area of freedom, security and justice,[122] and, more specifically, the area of **judicial cooperation in criminal matters and police cooperation** as laid down in Chapters 4 and 5 of Title V of Part 3 of the Treaty on the Functioning of the European Union (Articles 82 to 89 TFEU). This is relevant given the cross-border nature of the types of crime that law enforcement agencies use hacking techniques to investigate.
- Competence in the area of **data protection and privacy**, given the intrusive nature of hacking by law enforcement authorities.
    - based on Article 16(1) TFEU (right to the protection of personal data); and
    - based on Article 7 (respect for private and family life) and Article 8 (right to protection of personal data) of the Charter of Fundamental Rights of the EU, and also Article 11 (Freedom of expression and information).

Finally, the EU has a competence in the field of internal market and establishing a common commercial policy (133 Treaty on European Union – TEU). However, as legislation regulating the exports of hacking tools has already been adopted under this legal basis (the EU dual-use Regulation,[123] which is in the process of being updated[124]), this section will not further analyse this legal basis.

3.1. Judicial cooperation in criminal matters

The legal basis for the EU to act in the area of criminal justice is limited to the area of judicial cooperation in criminal matters and police cooperation as laid down in Title V of Part 3 of the TFEU. In this area, the following measures, which are further elaborated below, could potentially be adopted in relation to lawful hacking:

- Approximation of laws;
- Introduction of minimum standards; and
- Common investigative techniques.

Approximation of laws

Based on **Article 82(1) TFEU**, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, can:

a) adopt measures to lay down rules and procedures for ensuring recognition throughout the Union of all forms of judgements and judicial decisions;
b) prevent and settle conflicts of jurisdiction between Member States;
c) support the training of the judiciary and judicial staff; and
d) facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions.

[122] Art. 2 sub 2 (d) TFEU, art. 4(2)(j) TFEU.

[123] COUNCIL REGULATION (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

[124] European Commission. 2016. Commission proposes to modernise and strengthen controls on exports of dual-use items.

Under point a), the EU adopted Directive 2014/41/EU regarding the European Investigation Order in criminal matters.[125] This Directive includes provisions on the interception of communications (Chapter V and recitals 30 to 32), covering the collection of telecommunications content as well as associated traffic and location data. It does not, however, discuss the possibility for law enforcement agencies to use hacking techniques to facilitate the interception of communications.

Introduction of minimum standards

Based on **Article 82(2) TFEU,** the EU can introduce minimum standards, but only "to the extent necessary to facilitate mutual recognition of judgements and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension". Moreover, according to the provisions, the minimum standards may concern:

a) mutual admissibility of evidence between Member States;
b) the rights of individuals in criminal procedure;
c) the rights of victims in crime; and
d) any other specific aspects of criminal procedure that the Council has identified in advance by a decision (the so-called *passerelle* clause).

Thus, Article 82(2)(a) could, for example, include minimum standards on the admissibility of evidence gathered in a criminal investigation in which data pertaining to the accused are located on a server in another EU Member State and law enforcement agencies use hacking techniques to access such data.

Article 82(2)(b) appears less relevant, as the "minimum standards" in terms of the data protection rights of individuals (including suspects or accused persons) in criminal procedure are already regulated through EU data protection laws (see more detail in section 3.2).

Furthermore, Article 82(2)(c) does not appear relevant as victims in a crime would not be affected by law enforcement hacking practices.

Finally, regarding Article 82(2)(d), there has been no Decision by the Council that identifies "hacking by law enforcement" as an aspect of criminal procedure for which the European Parliament and the Council may establish minimum rules. However, if such a decision was to be taken by the Council, this could potentially provide for the EU legal basis to adopt measures on the use of hacking techniques by law enforcement.

No legislation has been adopted under this legal basis on how and when law enforcement may use hacking practices in cross-border situations. However, legislation including provisions on the interception of communications has already been adopted under Article 82 TFEU, such as Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims,[126] which allows the interception of communications and electronic surveillance (Article 9(4) and recital 15).

Beyond the scope of the TEU, the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union includes provisions on requesting assistance for interception, recording and transmission of telecommunications for a criminal investigation (Title III).[127]

---

[125] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041.

[126] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 20112 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA.

[127] Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union, 12 July 2000.

Minimum rules for definitions of criminal offences

Article 83 TFEU concerns the setting of **minimum rules for definitions of criminal offences** and sanctions in areas of serious crime with a cross-border dimension. However, in cybercrime, such a law has already been adopted; namely, the **EU Cybercrime Directive.**[128] The Cybercrime Directive aims to approximate the criminal law of the Member States regarding attacks against information systems by establishing minimum rules concerning the definition of criminal offences and relevant sanctions, as well as to improve cooperation between competent authorities (including law enforcement).

Common investigative techniques

Pursuant to **Article 87(2)(c) TFEU**, the EU may adopt legislation on common investigative techniques in relation to the detection of serious forms of organised crime. Hacking is an investigative technique and it could be useful for investigations into serious forms of organised crime such as the detection of large international child pornography rings, as well as drugs and/or human trafficking, etc.

Moreover, under **Article 87(3) TFEU**, the Council, acting in accordance with a special legislative procedure, may establish measures concerning operational cooperation between the police, customs, and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences.

3.2. Privacy and data protection

According to Article 51 of the **Charter of Fundamental Rights of the EU** (the Charter), EU institutions, bodies, offices and agencies must safeguard the fundamental rights provided for in the Charter, including the right to respect for private and family life (**Article 7**) and the right to data protection (**Article 8**). However, it should be noted that the Charter does not extend the competence of the EU to matters not included by the Treaties under its competence.

Moreover, EU primary law also contains a general EU competence to legislate on data protection matters, through **Article 16 TFEU**.

EU Charter of Fundamental Rights

Article 7 of the Charter states that "everyone has the right to respect for his or her private and family life, home and communications". Under this article, Member States are obliged to take all necessary measures to restrict the unlawful access to information by public authorities, as well as private parties.[129]

According to Article 53(3) Charter, if the right in the Charter corresponds to rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), the meaning and scope of those rights shall be the same as those laid down by the ECHR. In this case, Article 7 Charter corresponds to the rights guaranteed by Article 8 of the ECHR. Article 8(2) ECHR states in this regard that the right to private and family life cannot be restricted by a public authority "except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". For example, in the case *Malone v. UK*, the European Court of Human Rights (ECtHR) found that a system

[128] Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[129] http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf.

authorising the interception of communications to assist judicial police authorities was necessary to prevent disorder or crime, but could only be lawful and legitimate under the ECHR if the interference is in accordance with the law and it is necessary in a democratic society for the legitimate aim pursued.[130]

Moreover, Article 8 Charter establishes a specific fundamental right for data protection in EU law, stating that "everyone has the right to the protection of personal data concerning him or her". The article further states that personal data must be: i) processed fairly; ii) for specified purposes; iii) on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Article 8 also provides for the right of access to data which has been collected concerning a natural person and for the right to have it rectified. Finally, the article requires that compliance with data protection rules should be subject to control by an independent authority.

Article 11 Charter states that everyone has the right to freedom of expression and information, which includes the right to receive and impart information without interference by public authorities. The Court of Justice of the European Eunion also judged that this right is also applicable to electronic communications (see Joined Cases C-203/15 Tele2 Sverige AB v Post- och telestyrelsen) and C-698/15 (Watson, Brice & Lewis) v Secretary of State for the Home Department). This right coud be relevant when a person's communications are intercepted by law enforcement as part of a criminal investigation.

Article 16 TFEU

EU primary law also contains a general EU competence to legislate on data protection matters, through Article 16 TFEU. Article 16(2) TFEU mandates the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, to lay down the rules relating to the protection of individuals regarding the processing of personal data by the Member States when carrying out activities which fall within the scope of Union law (e.g. judicial cooperation in criminal matters), and the rules relating to the free movement of such data. Echoing Article 8 of the Charter, the article further states that compliance with these rules should be subject to the control of independent authorities.

EU law already adopted on the basis of Article 7 and 8 Charter and Article 16 TFEU

The relevant pieces of legislation already adopted on the basis of the relevant articles in the Charter and Article 16 TFEU are the:

- 2016 **General Data Protection Regulation** (GDPR)[131];
- 2016 **Directive on data protection in the police and justice sectors,**[132] which includes provisions on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

[130] Malone v. the United Kingdom (8691/79), judgement of 2 August 1984; See also: Eur. Ct. H.R., Kruslin v. France and Huvig v. France (Appl. Nos. 11801/85 and 11105/84), judgements of 24 April 1990, Rep. 1997-II.

[131] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[132] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

- **e-Privacy Directive,**[133] which includes provisions on the processing of personal data and the protection of privacy in the electronic communications sector.

Legal basis to further restrict privacy and data protection

Recital 73 of the GDPR states that restrictions may be imposed by EU or Member State law, as far as "necessary and proportionate in a democratic society to safeguard public security, including […] the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties".

In this regard, Article 23 GDPR specifies the purposes for which the EU or Member States law may restrict the scope of the obligations and rights provided for in the GDPR by way of a legislative measure. One of these purposes is when the restriction is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences. However, these restrictions should still respect the essence of the fundamental rights and freedoms. It should be noted that the safeguards in Article 23 GDPR only apply to national persons and therefore do not apply to situations where law enforcement is hacking industry computers.

Article 15(1) of the existing e-Privacy Directive allows Member States to adopt legislative measures to restrict the scope of privacy and data protection, "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences". Moreover, Article 11 of the proposed e-Privacy Regulation would also allow the EU or Member States to adopt law to restrict the scope of the privacy and data protection rights "where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society" to safeguard the prevention, investigation, detection or prosecution of criminal offence.[134] Contrary to Article 23 GDPR, the e-Privacy Directive does apply to legal persons, and provides a right to confidentiality of communications and protection of metadata of companies.

Based on these provisions and its competence regarding data protection (Article 16 TFEU), the EU could adopt further legislation specifying the ways in which the fundamental right to confidentiality of communications and data protection may be restricted for the purpose of criminal investigation, through the use of hacking tools by law enforcement. Article 23(2) GDPR states that such legislative measures need to contain the following specific provisions:

a) the purposes of the processing or categories of processing;
b) the categories of personal data;
c) the scope of the restrictions introduced;
d) the safeguards to prevent abuse or unlawful access or transfer;
e) the specification of the controller or categories of controllers;
f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
g) the risks to the rights and freedoms of data subjects; and
h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

[133] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. See also the Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.

[134] Article 11, COM(2017) 10 final (E-Privacy Directive proposal), in conjunction with Article 23 (1)(d) GDPR.

Legal basis to ensure adequate protection of data protection law

The preamble of the GDPR states that effective protection of personal data throughout the EU requires the **strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data**, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

Based on the EU legal basis regarding data protection, it could be argued that the EU would need to adopt further legislation clarifying the specific safeguards for individuals hacked by law enforcement (i.e. the right holders to the accessed computer systems) as part of a cross-border investigation in which law enforcement use hacking techniques. This would be to ensure a consistent level of protection for natural persons throughout the Union.

It should be noted that apart from the legislative measures mentioned above, the EU could also adopt **non-binding instruments**, in which it could clarify the rights in the Charter of Fundamental Rights and data protection legislation in the context of hacking as an investigative technique and identify appropriate safeguards to be included in the legal framework at national level.

In this regard, the EU could adopt:

- Recommendations;
- Opinions;
- Interinstitutional agreements;
- Resolutions;
- Conclusions;
- Communications;
- Green papers; and
- White papers.

In conclusion, this section has provided an initial scoping of the possible legal basis for the EU to legislate in the area of hacking by law enforcement. Although these lines of enquiry have been validated by EU-level stakeholders consulted for this study, these stakeholders stated that the debates on the topic were not mature enough to judge, firstly, whether EU legal intervention in the field is appropriate and, secondly, what the most appropriate or relevant legal basis would be.

To determine the full possibilities for EU intervention and to answer the question whether or not the EU has a clear legal basis to legislate on the use of hacking techniques by law enforcement would require a full legal basis analysis, given that this specific area would be a new field for the EU legislation. Such a legal basis analysis would also have to take into account any EU legislation and provisions already in place which are applicable to situations in which law enforcement are using hacking techniques as part of criminal investigations in the Member States. Moreover, as noted above, non-binding instruments may prove more appropriate for this area of limited EU competence.

However based on this initial scoping exercise, the following potential avenues for EU action seem worthy of further investigation:

- Minimum standards on the **mutual admissibility of evidence** gathered in a criminal investigation using hacking techniques, if necessary to facilitate mutual recognition of judgements and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension (Article 82(2) a TFEU);

- Legislation on **common investigative techniques** such as hacking techniques in relation to the detection of **serious forms of organised crime** (Article 87(2)(c) TFEU);
- Measures concerning **operational cooperation** on the use of hacking techniques, between the police, customs, and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences (Article 87(3) TFEU);
- Provisions on the **protection data protection rights** in cases where law enforcement are using hacking techniques (Art 16 TFEU, art. 7 and 8 EU Charter).

Finally, as stated above, the EU could potentially adopt minimum standards if the Council identifies "hacking by law enforcement" as a specific aspect of criminal procedure for which the European Parliament and the Council may establish minimum rules in accordance with Article Article 82(2)(d) TFEU.

4. MEMBER STATE LEGAL FRAMEWORKS FOR HACKING BY LAW ENFORCEMENT

Based on data collected across six EU Member States (see Appendix 1), this chapter presents a comparative analysis of Member State legislative frameworks, and the practical application of those frameworks, for hacking by law enforcement. Further comparative input is extracted from three non-EU country reports (see Appendix 2). This chapter is structured as follows:

Section 4.1. **Legal frameworks and context:** Overview of the status of hacking by law enforcement within existing and emerging Member State laws, and the contexts in which those laws were developed;

Section 4.2. **Provisions of the legal framework:** Focuses on the *ex-ante* conditions governing hacking by law enforcement and the subsequent *ex-post* mechanisms for oversight and supervision of these hacking practices;

Section 4.3. **Fundamental rights considerations:** Discusses the approaches of the six Member States to the protection of fundamental rights within the legislative process and application of hacking practices by law enforcement;

Section 4.4. **Technical means used by law enforcement:** To the extent possible, presents an assessment of the technical means for hacking by law enforcement as enshrined in law, as well as used in practice; and

Section 4.5. **Security and intelligence services:** Presents the legal rules and possibilities for hacking by the security services across the six Member States, to explore whether best practices from security service legal frameworks and practices can be used in the law enforcement sphere.

4.1. Legal frameworks and context

This section presents the study findings on the status of the legal framework for hacking by law enforcement, as well as the context in which these frameworks were developed, across the six Member States covered by this study. It explores the presence (or not) of specific legal frameworks that govern the use of hacking practices by law enforcement, highlighting examples from national level, before discussing the context in which the legislative provisions were adopted.

Status of specific legal frameworks for hacking by law enforcement

The use of hacking techniques by law enforcement, as discussed throughout this study, is a relatively new phenomenon. It is therefore not surprising, considering the notion of 'law lag',[135] that not all Member States examined have specific legislative provisions. Furthermore, those that do have specific legislative provisions have, for the most part, enacted them recently.

More specifically, four of the six Member States examined (France, Germany, Poland and the UK) have passed specific legal provisions related to the use of hacking techniques by law enforcement. As illustrated below, three of these four Member States passed these legislative changes in 2016.

[135] Law lag in this instance relates to the notion that the development and enactment of law is behind the related technological advancements.

Table 3: Specific legal provisions for law enforcement hacking in four Member States.

France Loi nº 2016-731, of 3 June 2016, amending section 6 of Chapter II of Title XXV of Book IV of the Code of Criminal Procedure (*Code de procédure pénale*). This amendment introduced the possibility for French law enforcement agencies to remotely access computer data, if certain conditions are met.
Germany Although no specific provisions exist in the German Code of Criminal Procedure (*Strafprozessordnung* – StPO), §20k(1) of the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz* – BKAG) explicitly permits the Federal Criminal Police Office to intervene with the technical means of information technology systems. Again, this is only possible if certain conditions are met. This provision was provided for in the 2008 revision of the Law, coming into force on 1 January 2009. Furthermore, even though no specific provisions exist, it is possible for law enforcement to use hacking techniques under the StPO. It is possible through 'annex competences' to provisions considered to be similar in nature to their digital counterparts (e.g. interception of telecommunications, §100a StPO).
Poland The Act of 15 January 2016 amending the Police Act and Certain Other Acts introduced remote access capabilities to the Polish legal lexicon. The amendments stipulate that the use of 'operation controls' is permitted to extract and record data from data storage media, telecommunications terminal equipment, information and communication systems.
United Kingdom In the UK, the specific governance of hacking by law enforcement is provided for in the Investigatory Powers Act, which came into effect in November 2016. The Investigatory Powers Act permits law enforcement to obtain data from devices by interfering with the associated electronic equipment – this provision is labelled 'equipment interference'.

However, as illustrated by Germany's use of 'annex competences' to the StPO, the absence of specific legislative provisions does not necessarily prohibit or prevent the use of hacking techniques by law enforcement. In fact, it is widely acknowledged that law enforcement agencies in Italy[136] and the Netherlands[137] (i.e. the two Member States examined that do not currently have specific legal provisions) use hacking techniques. The use of these so-called 'grey area'[138] legal provisions is not considered sufficient by the UN, which calls instead for legislative clarity and precision.[139]

In countries such as Italy and the Netherlands, the existing legal bases for the use of hacking techniques by law enforcement are tied to more traditional investigative tools that are considered similar. For example, within Italy's current Code of Criminal Procedure (*Codice di procedura penale*), the use of malware, if its aim is the interception of communications, is

[136] Citizen Lab. 2014. Mapping Hacking Team's "Untraceable" Spyware. Accessed on 28.02.17 at: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

[137] https://www.om.nl/vaste-onderdelen/zoeken/@85963/wereldwijde-actie/.

[138] Expert workshop conducted for this study.

[139] UN Human Rights Council. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40.

governed by the existing provisions for the interception of communications (Article 266[140]). These traditional interception tools (e.g. wiretapping) are considered to have a more limited potential for invasiveness compared with hacking techniques such as malware.[141]

Law enforcement in Australia and the US also implement hacking practices based on 'grey area' legal provisions, as detailed in Box 4, below.

Box 4: Non-EU countries: Use of 'grey area' legal provisions.

Australia

There is **no specific legal framework for the use of hacking by law enforcement** in Australia, and the legislation used to govern it has also not been publicly referenced.[142] However, whilst there is no legislation that mentions hacking by law enforcement specifically, inferences can and have been made regarding the most relevant Acts.[143]

These Acts include the **Telecommunications (Interception and Access) Act 1979** and the **Surveillance Devices Act 2004**.

United States

There is **no detailed piece of US legislation specifically regulating the use of hacking by law enforcement.**[144] Whilst federal statutes such as Part I of the Electronic Communications Act (ECPA) (1986)[145] – an expansion of the 'Wiretap Act' (1968)[146] – and the Stored Communications Act (SCA)[147] govern law enforcement surveillance of real-time and stored communications respectively, both statutes pre-date the use of government hacking.[148] Instead, although never expressing it as absolute policy,[149] law enforcement agencies have generally sought authorisation for the use of hacking in investigations in search and seizure warrants applied under Rule 41 of the Federal Rules of Criminal Procedure (Rule 41).[150]

With this said, a specific legal framework for hacking by law enforcement is on the agenda for discussion at the bipartisan Encryption Working Group (EWG) of the US Congress.[151]

Both Italy and the Netherlands, however, are in the process of providing specific legislation for the use of hacking tools (although the proposed laws are at very different stages of development). Table 4 outlines these legislative propositions.

---

[140] Galli, F. 2016. The interception of communication in France and Italy – what relevance for the development of English law? *The International Journal of Human Rights*. Volume 20(5).

[141] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

[142] Molnar, A. 2017. Expert interview conducted for this study.

[143] *Id.*

[144] Expert interview conducted for this study. 2017.

[145] 18 U.S.C. § 2510 – an expansion of the Wiretap Act to include digital communications.

[146] Omnibus Crime Control and Safe Streets Act (1968), P.L. 90-351, 801, 82 Stat. 197, 212 – provides the US government with procedural regulations surrounding the interception of real-time telecommunications.

[147] 18 U.S.C. Chapter 121 §§ 2701–2712.

[148] The first report of the US government possessing the capability to use remote hacking in an investigation was in 2001 – Thompson, R.M. (2016). Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Background on Amendment to Rule 41.

[149] Crump, C. (2017) Interview.

[150] Thompson, R.M. (2016). Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Congressional Research Service.

[151] House Judiciary Committee & House Energy and Commerce Committee Encryption Working Group. 2016. Encryption Working Group: Year-End Report. December 20, 2016.

Table 4: Specific legislative proposals tabled in Italy and the Netherlands regarding hacking by law enforcement.

Italy

Decisions from the Court of Cassation, in 2009 (Decision Nº 24695) and 2012 (Decision Nº 254865), validated the use of hacking tools by Italian law enforcement agencies for accessing stored data under the existing legal basis (i.e. without judicial approval). However, these precedents were, in effect, contradicted by a 2015 judgement of the Court of Cassation. This judgement ruled that specific conditions should be met if hacking tools are to be used for intercepting communications – e.g. the "surveillance should take place in clearly circumscribed places, identified at the outset, and not wherever the subject might be".[152] As a result of these discrepancies, a similar case in 2016 referred the issue to the 'Joint Sessions' (SS.UU.) – the most authoritative session of the Italian Court of Cassation. The outcome of the 'Joint Sessions' was that the use of hacking tools is permitted for serious crimes that fall within the concept of organised crime.

Furthermore, the decision separated the operational modes of hacking tools into two categories: 'online surveillance' and 'online search'. The former category relates to the interception of an information flow between devices (e.g. microphone, video, keyboard etc.) and the microprocessor of the target device. 'Online search' relates to copying the memory units of a computer system.[153]

In addition, since February 2015, four legislative proposals have been tabled, aiming to add specific legal provisions on the use of hacking tools by law enforcement. The first attempts were heavily criticised by the Italian Parliament; however, the most recent draft law – the so-called 'Quintarelli' draft law – was published in February 2017 and approaches legislation of the topic differently. Primarily, the approach is notable for its heavy technical insight into the diverse functionalities of trojans, the preferred tools of Italian law enforcement. Conditions included in this draft law are discussed further in section 4.2.

Netherlands

The Computer Crime III Bill, which is informally referred to as the Hacking Law, is a legislative proposal currently being considered by Dutch legislators. This Bill aims to regulate the use of hacking as an investigative power through explicit provisions related to remote searches through the use of policeware (i.e. police malware) and other forms of hacking.

The proposed law was announced by the Ministry of Security and Justice in 2012. This announcement was followed by a public consultation, launched in June 2013, before its submission to Parliament in December 2015. In December 2016 the Dutch Second Chamber voted in favour of adopting the proposed law. Subsequently, the Act will now be debated in the Senate.

Context for the development of legislative provisions

A range of interlinked factors are driving the development of specific legislative provisions for the use of hacking techniques by law enforcement agencies. These drivers include:

- Increasing **use of encryption** for communications, as well as stored data – this is reported to be a considerable barrier to law enforcement investigations;

[152] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

[153] *Id.*, p. 5.

- Threat of **terrorism and organised crime**; and
- **Criticisms of government surveillance** related to violations of the fundamental right to privacy.

On the first point, and as discussed in greater detail in section 2.1, encryption has been a recurring subject of debate over recent decades. The so-called 'Crypto Wars' of the 1990s were characterised by the attempts of the US and other governments to develop the ability to decrypt all encrypted data. Examples of these attempts include the proposed 'key escrow' system and the restrictions placed through US export controls on the strength of encryption technologies. However, these attempts were strongly opposed; 'key escrow' was dropped and export controls were relaxed following significant criticism of their impact on US competitiveness.[154]

In the years since, international consensus has emerged supporting the development and adoption of strong encryption capabilities and the avoidance of 'backdoors'. The UN Special Rapporteur for the Human Rights Council,[155] Europol and ENISA[156] are some of the international and regional bodies supporting this stance.

As clearly stated in a Europol and ENISA Joint Statement on the topic, hacking techniques, when used by law enforcement agencies, are privacy-invasive investigative tools. The Joint Statement further states that the use of such tools should not "intentionally weaken technical protection mechanisms"[157] and that "legislation [on the topic] must explicitly stipulate the conditions under which law enforcement can operate".[158]

In contrast to this support on the EU level, however, recent rhetorical statements by national-level politicians have raised concerns regarding the increasing prevalence of encryption as an investigative barrier, as illustrated in Box 5. As such, the prominence of encryption in the modern world has driven the adoption of specific legal provisions to govern the ability to circumvent encryption technologies under certain conditions.

Box 5: Member State statements on encryption as an investigative barrier.

France and Germany

In a 2016 joint speech, the French and German Interior Ministers, Bernard Cazeneuve and Thomas de Maizière, recognised the importance of strong encryption to society whilst simultaneously highlighting the increasing challenge encryption poses to law enforcement agencies. Continuing this point, Cazeneuve and de Maizière insisted that encrypted communications must be available to law enforcement.[159]

United Kingdom

A group of security experts from the Computer Science and Artificial Intelligence Laboratory at the Massachusetts Institute of Technology reported that former UK Prime Minister, David

[154] Open Technology Institute. 2015. Doomed to repeat history? Lessons from the Crypto Wars of the 1990s.

[155] UN Human Rights Council. 2015. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/29/32.

[156] Europol and ENISA. 2016. On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement. 20 May 2016.

[157] *Id.*

[158] *Id.*

[159] Franco-German initiative on internal security in Europe. 2016. Speech by Bernard Cazeneuve, French Minister of the Interior, and Thomas de Maizière, Minister of the Interior of the Federal Republic of Germany on 23 August 2016, Paris. Accessed on 01.02.17 at: http://www.interieur.gouv.fr/Archives/Archives-ministre-de-l-interieur/Archives-Bernard-Cazeneuve-avril-2014-decembre-2016/Interventions-du-ministre/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe.

Cameron, "simply wants the police to have access to everything".[160] This statement came in the wake of a Cameron speech delivered in the wake of the Charlie Hebdo murders in Paris. Cameron's speech asked and answered as follows:

"are we going to allow a means of communications where it is simply not possible to [read it]? My answer to that question is: no, we must not."[161]

Various law enforcement / judiciary personnel (France, Spain, the UK and the US)
In August 2015, the Paris chief prosecutor (François Molins), the commissioner of the City of London Police (Adrian Leppard), the chief prosecutor of the High Court of Spain (Javier Zaragoza) and the Manhattan district attorney (Cyrus R. Vance Jr.) penned an op-ed for the *New York Times* entitled 'When Phone Encryption Blocks Justice'.[162] This article argues that the increasing prevalence of full-disk encryption on mobile phones results in impunity and, at the minimum, hinders investigations.[163]

Furthermore, law enforcement concern over the use of encryption ties into the second contextual driver, the **threat of terrorism and organised crime**. The UN High Commissioner for Human Rights stated in a 2014 report that "governments frequently justify digital communications surveillance programmes on the ground of national security, including the risks posed by terrorism".

As such, several of the specific provisions installed to govern the use of hacking techniques by law enforcement were passed under the auspices of legislation developed for the fight against organised crime and terrorism. For example, the amendments to the French Code of Criminal Procedure were introduced via Loi n° 2016-731 of 3 June 2016 strengthening the fight against organised crime, terrorism and their financing. Moreover, the UK's Investigatory Powers Act was introduced because of the findings of the Independent Reviewer of Terrorism Legislation, David Anderson QC.

Furthermore, terrorism is a key driver of law enforcement hacking practices in non-EU countries, such as Israel.

Box 6: Non-EU countries: Terrorism as a driver of hacking by law enforcement

Israel
The use of hacking techniques by Israeli law enforcement agencies is reportedly a frontline defence against terrorist activities. In 2010, for instance, the Israeli government afforded law enforcement and security agencies greater investigative powers with the primary aim of tackling terrorist use of the internet.

This last example illustrates the links between the first two contextual drivers and the third, as David Anderson QC, within his role as Independent Reviewer of Terrorism Legislation, was tasked with reviewing the operation and regulation of the UK's investigatory powers. This

[160] Abelson, H. et al. 2015. Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. *Computer Science and Artificial Intelligence Laboratory Technical Report.*

[161] Cameron, D. 2015. PM: spy agencies need more powers to protect Britain, Jan. [Online]. Available: https://embed.theguardian.com/embed/video/uk-news/video/2015/jan/12/david-cameron-spy-agencies-britain-video.

[162] Vance, C. Y., Molins, F., Leppard, A. and Zaragoza, J. 2015. When Phone Encryption Blocks Justice. The Opinion Pages. *The New York Times*, August 11, 2015.

[163] *Id.*

task came amid **widespread criticism of the use of surveillance capabilities**, as prompted by the Snowden revelations.[164]

Further to the criticisms, the Investigatory Powers Tribunal, established by the Investigatory Powers Act, has ruled that many UK security services have been collecting data unlawfully for many years. Although not specifically related to law enforcement use of hacking techniques, these revelations describe a context in which governments are being challenged for their use of such capabilities – thus driving the need for specific legislation on how these powers can be used across both the security services and law enforcement.

4.2. Provisions of the legal framework

This section delves deeper into the provisions of the legal frameworks outlined above. It first presents the study findings on the *ex-ante* conditions that are included in the legal provisions and need to be met for law enforcement hacking to be permitted, before examining the *ex-post* considerations that provide for supervision and oversight after the hacking practices have been undertaken.

Ex-ante considerations

As discussed in chapter 2, the *ex-ante* conditions governing hacking by law enforcement have been the subject of repeated recommendations by multiple UN bodies. To a certain extent, these explicit recommendations have **served to align the types of conditions included within the existing and proposed legal frameworks** of the six Member States examined.

Considering the conditions that must be met for the lawful restriction of the right to privacy (see Box 7), the abovementioned UN recommendations aim to ensure that appropriate *ex-ante* judicial authorisation is in place for hacking by law enforcement. Consequently, these recommendations also discuss the inputs to, and the decision-making process for, this judicial authorisation.[165,166]

Box 7: Conditions for the lawful restriction of the right to privacy.

EU Charter on Fundamental Rights – Article 52

Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the **principle of proportionality**, limitations may be made only if they are **necessary** and genuinely **meet objectives of general interest** recognised by the Union or the need to protect the rights and freedoms of others.

European Convention on Human Rights – Article 8

There shall be no interference by a public authority with the exercise of this right **except** such as is **in accordance with the law** and is **necessary** in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[164] Milmo, C. 2014. Edward Snowden revelations: GCHQ 'using online viruses and honey traps to discredit targets'. Article in *The Independent*. Accessed on 03.03.17 at: http://www.independent.co.uk/news/uk/home-news/edward-snowden-revelations-gchq-using-online-viruses-and-honey-traps-to-discredit-targets-9117683.html.

[165] UN High Commissioner for Human Rights. 2014. The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/27/37.

[166] UN Human Rights Council. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40.

Proposal for Regulation on Privacy and Electronic Communications (e-Privacy Regulation) – Article 11

Union or Member State law may restrict […] where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.

Thus, the existing or proposed legal frameworks in all Member States examined have, in some form or other, authorisation prior to law enforcement hacking practices (see Table 5).

Table 5: Legal provisions for judicial authorisation of hacking by law enforcement

France
The use of hacking techniques by law enforcement is subject to authorisation by either the judge of freedoms and detention (*le juge des libertés et de la détention*) or the investigating judge (*juge d'instruction*) on the application of the public prosecutor (706-102-1 and 706-102-2 of the Code of Criminal Procedure).

Germany
Court authorisation is required for hacking practices (§100a StPO and §20k BKAG) in response to a request from the public prosecutor's office. However, in exigent circumstances, the provisions allow for the public prosecutor to issue such an order without prior court authorisation if the order is confirmed by the court within three days.

Italy
Law enforcement authorisation for the use of hacking tools must be obtained from the public prosecutor and subsequently validated by the judge presiding over the preliminary investigation ('Quintarelli' draft law amending title III of Book III of the Code of Criminal Procedure).

Netherlands
The public prosecutor is required to submit a written request for prior authorisation to the investigative judge, before hacking practices can be conducted by law enforcement agencies (Article 126nba (4) Code of Criminal Procedure, as proposed in the Computer Crime III Bill).

Poland
Hacking practices require prior authorisation by a district court, generally courts of second instance (Article 19 §1 Police Act). The process for authorisation is complicated and requires input from three actors: a high-ranking police officer needs to obtain permission from the prosecutor to then request authorisation from the court. Similar to Germany, law enforcement may undertake hacking practices without prior authorisation in urgent circumstances if consent is granted by the court within five days.

United Kingdom
To engage in hacking practices, national law enforcement must be issued an equipment interference warrant by the appropriate law enforcement chief. This warrant must also be approved by a Judicial Commissioner – a role created for the purposes of the Investigatory Powers Act. This process is known as a double-lock authorisation safeguard. However, in

urgent circumstances, the law enforcement chief can order the hacking practices with subsequent authorisation by the Judicial Commissioner within three working days.

Table 6: Non-EU countries: Legal provisions for judicial authorisation of hacking by law enforcement

Australia In both the Telecommunications (Interception and Access) Act and the Surveillance Devices Act, a warrant, issued by a judge or a member of the Administrative Appeals Tribunal, is required at the request of law enforcement.
Israel In 2010, the Israeli government expanded law enforcement investigative powers in relation to digital data collection. Under the new provisions, law enforcement must request authorisation from a court.
United States A search warrant, issued under Rule 41, is required for law enforcement to conduct hacking practices. Such a warrant must be authorised prior to the hacking by a magistrate or district judge.

As suggested in Table 4, all countries require *ex-ante* judicial authorisation for police hacking, demonstrating the seriousness of the privacy infringement. Legislation does acknowledge that urgent or exigent circumstances may sometimes demand that the receipt of prior authorisation is not necessary; however, Member States still require that judicial authorisation is subsequently obtained.

In Germany and the UK, for example, the time period for obtaining subsequent authorisation is three days. In Poland, however, it is longer, at five days – a provision that was questioned by the Council of Europe's Venice Commission. The Venice Commission was tasked by the Chair of the Parliamentary Assembly's Monitoring Committee to examine the amendments to the Polish Police Act. In its critique, the Venice Commission stated that, although the Polish authorities assured otherwise, these legal provisions could be interpreted to allow the short-term use of hacking practices by law enforcement (i.e. within the five-day limit) free from judicial control. As such, it urged a reconsideration of this provision, suggesting that authorisation in urgent circumstances should be required in fewer than five days.

For authorisation to be permitted, the legal provisions across all Member States examined require that requests for the use of hacking techniques meet **certain conditions**. These conditions aim to ensure that hacking practices are only used to restrict the right to privacy when in line with Article 8 of the European Convention on Human Rights (i.e. that they are necessary and proportional and follow legitimate aims). The path to determining necessity and proportionality in these instances differs across all Member States; however, many of the inputs used to reach such a decision (i.e. the *ex-ante* conditions) are similar in nature.

An *ex-ante* condition found in the legislative provisions of all six Member States relates to **restricting the use of hacking tools to investigations related to crimes of a certain gravity**. In some Member States, the legislation presents a specific list of crimes for which hacking is permitted; in others, the limit is set for crimes that have a maximum custodial sentence of greater than a certain number of years – different Member States have a different number of years.

Regarding the former type of legislative provision, the Italian draft law permits the use of hacking tools for organised crime investigations only. Furthermore, §100a(2) of the German StPO provides a concrete list of offences that are considered serious.

Regarding the latter type of legislative provision, the use of hacking techniques in the Netherlands (as dictated by Article 126nba (1) can only be requested for investigations into crimes described in Article 67(1) of the Dutch Criminal Code of Procedure. Article 67(1) details crimes with a maximum custodial sentence of four years or more (besides some specifically designated offences with a lower maximum); moreover, besides the seriousness of the crime in the abstract, the crime in the specific case must be determined to seriously breach the rule of law.

Other *ex-ante* conditions that are common across the Member States include limiting the duration of the hacking practices; ensuring the hacking practices are appropriately targeted; stipulating the key information that should be included in a request for authorisation; and separating authorisation for different functionalities of a hacking tool. Examples of these conditions are included in Table 5.

Table 7: Examples of *ex-ante* conditions for authorisation of hacking practices.

Limiting the duration of hacking practices
In **France**, hacking techniques are permitted under Articles 706-102-1 and 706-102-2 of the Code of Criminal Procedure. Under 706-102-1, operations can only be authorised for a maximum period of one month. Renewal is possible once under the same conditions. Under 706-102-2, operations are permitted for a longer duration, up to a maximum initial period of four months, renewable under the same conditions up to a total of two years. The governance differs under these provisions as Article 706-102-1 relates to investigations led by the public prosecutor, whereas 706-102-2 relates to investigations led by the investigating judge.
German legislation permits the use of hacking techniques up to three months (§20k, BKAG). This can be extended for a subsequent maximum period of three months. Furthermore, the measure must be terminated immediately if the conditions of the order are no longer fulfilled.
Ensuring hacking practices are targeted
German legislative provisions require suspicion of an individual based on certain facts and §100a(3) stipulates that such an order for the use of hacking tools to facilitate the interception of telecommunications must be targeted only against the suspect or against persons whom it can be assumed are communicating with the suspect.
In the **Netherlands**, the proposed Computer Crime III Act requires that the alleged crime, the name (if known) of the suspect and the number of the computerised device to be hacked are all included in the request for authorisation of hacking techniques; only devices in use by the suspect can be hacked.
In the **US**, the concept of 'particularity' is strong regarding the issuing of a warrant in line with the Fourth Amendment. This concept states that the law enforcement officers must describe the target of the warrant.

Information to be included in the request for authorisation

Beyond the inclusion of the abovementioned details, the proposed **Dutch** legislative provisions require that requests for authorisation for the use of hacking techniques by law enforcement include a range of important data. These include the circumstances which show that the crime to be investigated is a serious breach of law and that the investigation needs the use of hacking practices urgently; a description of the type and functionality of the technical means to be used; the purpose of the hacking; which part of the computer and which category of data are to be accessed; and the time or time period.

In **Poland**, Article 19 §7 of the Police Act stipulates that a request for the use of hacking techniques requires details such as: a description of the crime; a justification of the necessity of the techniques, including an assessment of other means; personal data or other data facilitating the unambiguous determination of the targeted entity or object; and the objective, time and type of hacking techniques to be employed.

In **Australia**, under the assumed 'grey area' legal provisions, law enforcement must apply for a warrant. Such an application should include the context of the investigation, the period for which the warrant would be in force and details regarding why the period is necessary.

Separating authorisation for different hacking functionalities

The **French** legislative provisions governing the use of hacking techniques by law enforcement further stipulate that each type of hacking requires its own authorisation.

Italy's draft law aims to separate the varied functions of hacking tools, such as the ability to track targets and intercept the communications of targets. As such, separate authorisation requests are required for each functionality and, as will be detailed further in the next section, the use of these different functionalities is monitored.

Beyond these more common provisions, the Member States examined stipulate a range of additional, rarer provisions. For example:

- **Deletion of non-relevant data**. In Germany, data concerning the core area of the private life is regarded as off-limits and inadmissible – StPO §100a (4). This subsection states that these data shall not be used, shall be deleted without delay and the fact that they were obtained and deleted shall be documented, with a view to notification (§101 StPO). This provision is also provided for in section 20k (7) of the BKAG, which states that, as far as possible, data related to the core area of private life should not be collected, and data that are collected must be screened and deleted by the Federal Data Protection Supervisor and two other members of the Federal Criminal Police Office.
- **Provisions to ensure the appropriateness of the hacking tools used by law enforcement.** Under the proposed **Italian** law, trojans to be used by law enforcement must be directly operated by law enforcement and not by private contractors. Furthermore, every operation that uses a trojan must be duly logged and documented in a tamperproof, verifiable way; and once installed, a trojan shall not reduce the security of a device. Similarly, §20k of the **German BKAG** stipulates that key information related to the technical means used shall be logged. Namely, the information to be logged includes: the designation of the technical means and its date of use; the organisational unit implementing the action; and information related to the identification of the target system and the collected data. In the **Netherlands**, an Order in Council will stipulate rules on the authorisation and expertise of the investigating officers that can be tasked with hacking and art. 126nba (8) (b) stipulates that activities must be logged and included in the Order in Council. These provisions are some of the only specific legal provisions

which take into account the risks posed by law enforcement hacking to the security of the internet.

The *ex-ante* conditions described above provide the basis on which a decision is taken (considering the principles of necessity and proportionality) on the use of hacking techniques by law enforcement. In addition to these inputs, many Member States make specific reference to these principles within their legislative provisions. For instance, in the Netherlands, the public prosecutor's request, as well as the decision of the investigative judge, must be based on a proportionality assessment. Furthermore, advice is provided to investigative judges by a Central Review Commission. In Poland, the request for authorisation is required to stipulate the necessity of the use of hacking techniques and the *'article préliminaire'* of the French Code of Criminal Procedure states that coercive measures, such as the use of hacking techniques, must be "strictly limited to the needs of the process, proportionate to the gravity of the offence charged and not such as to infringe human dignity".

In conclusion, these provisions, when aggregated, echo Article 8 of the European Convention on Human Rights, as well as the UN recommendations, which call for safeguards related to the nature, scope and duration of possible measures, and paragraph 95 of the ECtHR judgement in *Saravia v Germany*[167]. In other words, they provide a good basis of information to the judiciary on which to decide whether the use of hacking techniques should be permitted in any given situation. However, there are many and varied criticisms of the suite of conditions provided for in the different national laws and the extent to which they protect the fundamental right to privacy. These will be discussed further in section 4.3.

Ex-post considerations

In contrast to the *ex-ante* conditions and considerations, international recommendations for oversight and supervision of hacking practices 'after the fact' have been less common and less detailed. As a result, unlike with the *ex-ante* conditions, the six Member States examined present a wider variety of mechanisms to provide *ex-post* transparency and accountability.

With that said, two interlinked mechanisms are in place across most Member States: i) the requirement to notify targets of law enforcement hacking techniques; and ii) the requirement to ensure the right to effective remedy for targets of law enforcement hacking techniques.

- The Dutch Computer Crime III Bill requires that, as soon as the interest of the investigation allows, targets of hacking are notified and have the opportunity to challenge hacking orders in court. Under certain circumstances, however, notification may be omitted if this is 'reasonably not possible'.
- In Germany, StPO §101 stipulates the legal requirement to notify persons targeted by an interception order, which may be facilitated by the use of hacking techniques. StPO §101 (5) states that "notification shall take place as soon as it can be effected" without endangering the investigation, persons involved or significant assets.
- The 2016 amendments to the Polish Police Act provide targets of hacking practices with the opportunity to challenge the lawfulness of an operation within the scope of the criminal proceedings.

These mechanisms are further supported by the presence of details related to the use of hacking techniques in the investigation file, which will be provided to the suspect at trial.

Beyond these two mechanisms of *ex-post* transparency, the conditions stipulated by Member States become more varied.

[167] Case 54934/00.

Some Member States implement varying provisions related to oversight of the technical elements of the hacking techniques. Others provide for higher-level reporting or review mechanisms. Examples of both types of *ex-post* mechanism are provided in Table 8.

Table 8: Member State approaches to ex-post supervision and oversight of hacking by law enforcement.

Provisions related to oversight of the technical elements

The legislative provisions in **Italy, the Netherlands** and **Germany**, for instance, stipulate that the technical means used by law enforcement must be removed from the target device. For instance, in the Netherlands, art. 126nba (6) of the Computer Crime III Bill requires that once the operation has ended, the hacking tool (e.g. trojan) needs to be removed. If it cannot be (completely) removed and removal poses risks to the functioning of the hacked computer, the public prosecutor shall inform the computer owner/administrator and provide sufficient information to enable him to completely remove the tool (e.g. trojan).

As detailed under *ex-ante* provisions, several Member States include provisions for logging details of a hacking operation. These provisions are also relevant as *ex-post* provisions. For instance, §20k of the **German BKAG** stipulates that key information related to the technical means used shall be logged. Namely, the information to be logged includes: the designation of the technical means and its date of use; the organisational unit implementing the action; and information related to the identification of the target system and the collected data. Similar provisions are included in the draft **Italian** law and **French** legislation.

Furthermore, the **Italian draft law** aims to safeguard the use of hacking tools through a range of innovative provisions, described as "astonishingly sensible"[168] by a critic of law enforcement use of hacking tools. These provisions stipulate that trojan production and use must be traceable through a National Trojan Registry, which would hold a 'fingerprint' of each version of the software. In addition, a trojan's source code must be deposited to a specific authority and must be verifiable with a reproducible build process (in a similar fashion to Debian Linux). Lastly, trojans must hold an annually reviewed certificate to ensure continued compliance with law and technical regulation.

These provisions act to help manage the risks posed by law enforcement hacking to the security of the internet.

Provisions for review / reporting

Article 19 §22 of the **Polish Police Act** states that "the Minister competent for internal affairs shall provide the lower (Sejm) and upper (Senat) chambers of the Parliament with information" about operational control annually. In addition, as per Article 19 §16a and 16b, the Police Commander in Chief is required to keep a "central register of requests and orders concerning operational control run by the Police authorities".

In **Germany**, as detailed in StPO §100b (5) and (6), all Länder and the Federal Public Prosecutor General are required to submit an annual report to the Federal Office of Justice. These reports should include: i) the number of proceedings in which telecommunications interception measures were ordered; ii) the number of orders; and iii) the underlying criminal offence of the proceedings. The Federal Office of Justice is then required to produce a country-wide summary of these measures. These data are publicly available. Furthermore, pursuant to §100e, the Federal Government has a duty to annually report a selection of data

[168] Moody, G. 2017. Italy Proposes Astonishingly Sensible Rules to Regulate Government Hacking Using Trojans. Accessed on 28.02.17 at: https://www.techdirt.com/articles/20170216/03431236726/italy-proposes-astonishingly-sensible-rules-to-regulate-government-hacking-using-trojans.shtml.

points to the Federal Parliament. These data, amongst others, include the number of surveillance measures, the duration of each surveillance measure, whether persons concerned were informed and whether the surveillance produced results of relevance to the criminal proceedings. However, these reporting obligations relate to surveillance measures more widely, of which only part will involve the use of hacking techniques.

The **UK's Investigatory Powers Act** stipulates the roles of two reviewers: the Investigatory Powers Commissioner and the Investigatory Powers Tribunal. The former reviews all cases of hacking by law enforcement to ensure that the *ex-ante* conditions were met and fundamental rights were considered; the latter is independent of the government – comprising members of the judiciary and senior members of the legal profession – and reviews all disputes and complaints related to hacking by law enforcement.

In **conclusion**, all Member States examined have measures in place to ensure supervision and oversight of the use of hacking techniques by law enforcement agencies. Of primary importance are the mechanisms for notification and effective remedy, which are prevalent across the Member States. Beyond these two approaches, however, the design and type of these supervision and oversight mechanisms vary greatly across the Member States. Although much variety exists, these mechanisms have been grouped into two areas, above, based on their aims: i.e. provisions related to the monitoring of the technical means for hacking; and provisions for review or reporting on the use of hacking techniques by law enforcement.

4.3. Fundamental rights considerations

This section discusses the fundamental rights considerations related to law enforcement's use of hacking techniques. Based on the provisions and conditions detailed above, this section highlights the criticisms and good practice elements of current and future legislation from a fundamental rights perspective.

As discussed above, the use of hacking techniques is purported to bring significant improvements in investigative efficiency and effectiveness and the inability to use such tools could, to a certain degree, result in impunity. However, this use of hacking techniques is inherently intertwined with the fundamental right to privacy. These techniques are extremely invasive when compared with traditionally invasive investigative tools such as wiretapping. As such, they severely restrict the fundamental right to privacy, as enshrined in the EU Charter (Article 7) and the European Convention on Human Rights (Article 8). This restriction is lawful only if certain safeguards are in place and specific conditions are met. As detailed in Box 7, above, any limitation on the exercise of the right to privacy must be:

- Provided for by law;
- Subject to the principle of proportionality; and
- Necessary.

Therefore, the first port of call is whether this restriction is **provided for by law**. As illustrated by the above sections, four of the Member States examined (France, Germany, Poland and the UK) have specific legal provisions for the use of hacking techniques and the legal restriction of the right to privacy. The other Member States (Italy and the Netherlands) are in the process of enacting specific legislation, although both have previously used hacking techniques with the support of non-specific legal bases intended for less invasive investigative tools.

Views differ on whether these 'grey area' legal provisions are sufficient to protect fundamental rights. The US Congressional Research Service reported in 2016 that national

laws relating to interception cannot appropriately govern tools with increased invasiveness[169] but, in many situations, national-level decisions have supported the use of the existing legislative provisions to authorise the use of hacking techniques.

In Italy, for example, case law from 2009 and 2012 supported the use of hacking techniques by law enforcement without a judicial warrant under existing legal provisions. Furthermore, to widespread criticism,[170] the Minister of Security and Justice in the Netherlands confirmed that Dutch police used Article 125i of the Code of Criminal Procedure (related to searching a premises with the aim of securing data stored on a computer) to justify the use of hacking techniques in an investigation.[171]

However, in Italy, subsequent judgements of the Court of Cassation contradicted elements of the 2009 and 2012 decisions leading to 'Joint Sessions'. These Sessions, aimed to reconcile the decisions and multiple attempts to specify the use of hacking techniques through legislation, have since occurred. These national-level developments suggest that Member States recognise the need to have specific legislative provisions and, with the Charter and Convention in mind, that these 'grey area' laws provide insufficient protection for the right to privacy.

Beyond the existence of specific legislation, any limitation on the right to privacy must be **subject to the principle of proportionality and the requirement of necessity**. As described by privacy organisations and global experts, the principle of proportionality ensures that the aim of the investigative tool to be employed is proportionate to the "sensitivity of the information accessed and the severity of the infringement on human rights".[172] The requirement of necessity states that the use of hacking techniques should be limited to situations where they are "strictly and demonstrably necessary to achieve a legitimate aim".[173]

Many of the elements that contribute to the application of these principles are important elements of Member State legal provisions, as described above. These include:

- ***Ex-ante* conditions:** judicial authorisation; limiting the use of hacking techniques to crimes of a substantial gravity; ensuring hacking practices are appropriately targeted; limiting the duration of a hacking practice; separating the authorisation for different functions of hacking tools; taking steps to ensure the appropriateness of the tools used; and the deletion of non-relevant or private data.
- ***Ex-post* mechanisms:** the notification of targets; the opportunity for effective remedy; provisions for review and reporting of the use of hacking techniques; provisions on removal of the hacking tool after use; and provisions related to oversight of technical elements of the hacking techniques.

However, the combinations of conditions and mechanisms differ across the six Member States examined, as does their implementation. In view of this, it has been questioned in many countries whether the particular set of conditions in the country would offer sufficient

---

[169] Thompson, R.M. 2016. Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Congressional Research Service.

[170] http://leidenlawblog.nl/articles/hacking-without-a-legal-basis.

[171] Vragen van de leden Berndsen-Jansen en Verhoeven (beiden D66) aan de Minister van Veiligheid en Justitie over het hacken van servers door de politie terwijl de zogenaamde «hackwet» nog niet door de Kamer is behandeld (ingezonden 26 augustus 2014). Antwoord van Minister Opstelten (Veiligheid en Justitie) (ontvangen 20 oktober 2014). Zie ook Aanhangsel Handelingen, vergaderjaar 2013–2014, nr. 34. Available here: https://zoek.officielebekendmakingen.nl/ah-tk-20142015-286.html.

[172] The International Principles on the Application of Human Rights to Communications Surveillance. 2013. Necessary and Proportionate. Accessed on 03.03.17 at: https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf.

[173] *Id.*

safeguards in light of the severe privacy intrusion. A long list of criticisms have been levied at the legal provisions of the Member States. A selection of these are represented in Table 9.

Table 9: Selected criticisms of Member State legal provisions for the use of hacking techniques by law enforcement agencies.

Criticisms related to the limits based on the gravity of crimes
Netherlands: A Dutch NGO points to inconsistencies within the Computer Crime III Bill. In its preamble, the Act states that hacking practices should only be used in exceptional cases (i.e. terrorism and cybercrime). In the legal provisions, however, these investigative powers can be used for any criminal offence which carries a maximum custodial sanction of four or more years in prison. This limit includes much more than terrorism and cybercrime.[174]
France: A representative of the French judiciary recognised that, in cases that require technical hacking support from the Centre for Technical Assistance (as governed by Articles 230-1 and 230-2), the use of hacking techniques is feasible for crimes with a potential custodial sentence of only two years.[175]
Poland: The Council of Europe's Venice Commission stated that the list of crimes included in the Polish legislative provisions is "quite broad".[176] It is further explained that, theoretically, hacking techniques could be used for relatively minor offences that fall within the broader fields mentioned (e.g. drug-related offences).
Criticisms related to notification of targets and effective remedy
Italy: It is reported by an academic expert that the use of hacking techniques and tools, and the evidence gathered through these means, is not challenged in court as many legal professionals do not have the required knowledge.[177] This inability to challenge the evidence collected limits the ability of targeted persons to gain effective remedy.
Netherlands: Although notification of targets of law enforcement hacking practices is legally stipulated, it is reported by Dutch civil society that it does not happen in practice.[178] This reportedly occurs when a law enforcement agency purchases hacking software from a private company and, as a result, signs a Non-Disclosure Agreement (NDA) preventing the release of information about the use of the hacking software. As such, notification of the target does not occur, limiting the ability for these targeted individuals to challenge these investigative practices and receive effective remedy.
Additional criticisms
Germany: The German legal framework contains provisions for the screening and deletion of data collected that relate to the core area of private life. However, a 2016 Constitutional Court ruling stated that the current safeguards for screening and deletion of these data are insufficient. It further recommends that these data need to be screened by an independent body.

[174] Siedsma, T. (Bits of Freedom). 2017. Expert interview conducted for this study.

[175] Legrand, E. 2017. Expert interview conducted for this study.

[176] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016, p. 13.

[177] Ziccardi, G. 2017. Expert interview conducted for this study.

[178] Siedsma, T. (Bits of Freedom). 2017. Expert interview conducted for this study; see also for more general evidence on Dutch notification practices: WODC, De Wet bijzondere opsporingsbevoegdheden – eindevaluatie, 2004. P.145. Available here: https://www.wodc.nl/binaries/ob222-volledige-tekst_tcm28-74925.pdf.

Italy: Deletion of non-relevant data is required under the proposed Italian law. However, it does not provide for the fact that law enforcement may already be cognisant of these data prior to deletion. Such data, although subsequently deleted, may support the investigation (i.e. the 'fruit of the poisoned tree' doctrine).

Netherlands: Further criticisms of the proposed Dutch legislation include the broad nature of the term 'computer', as included in the law. At present, this term may also include smart devices such as car operating systems and other IoT devices.[179]

Poland: The Council of Europe's Venice Commission criticised the maximum length allowed for hacking techniques (i.e. the duration), stating that it is "quite long".[180]

Beyond these criticisms related to specific conditions or mechanisms, there are significant criticisms across many of the Member States examined regarding the authorisation process which attempts to determine whether the use of such hacking techniques is legally permitted.

- In the **UK**, the civil society group Liberty raised significant concerns about the authorisation process detailed in the Investigatory Powers Act. Liberty stated that "the safeguards remain resolutely inadequate"[181] as the powers of the Judicial Commissioner, who is required to authorise the warrant for equipment interference, are "so circumscribed that the [Act] risks creating the illusion of judicial control over surveillance".[182]
- The **Polish** provisions for authorisation of hacking practices have attracted criticism from the Venice Commission and legal analysts. The Venice Commission stated that, although the Polish authorities assured otherwise, the legal provisions could be interpreted to allow the short-term use of hacking practices by law enforcement (i.e. within the five-day limit) free from judicial control.[183] Therefore, it urges a reconsideration of this provision.

  In addition, legal analysts have noted that, for authorisation, law enforcement agencies are required to provide materials justifying the action. However, they have suggested that the obligation to submit supporting materials (and not all available materials) renders substantive control incomplete. What follows is a situation where approximately 94% of all requests across Poland have been authorised, with some courts authorising 100% of requests.[184]
- Potentially a contributing factor to the above situation is the fact that a range of stakeholders have reported that the judiciary across several Member States (including **France, Germany, Italy and the Netherlands**) have a lack of knowledge on the hacking techniques they are authorising. This carries a risk of abuse of investigative power and complements arguments made by the UN Special Rapporteur for Privacy that stakeholders heavily involved in the legislative developments and debates on this topic do not fully understand the technical aspects of the issue (see section 2.1 for more detail).

[179] Koops, B.J., C. Conings & F. Verbruggen. 2016. Zoeken in computers naar Nederlands en Belgisch recht. Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?, Oisterwijk: Wolf Legal Publishers, pp. 51-60.

[180] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016, p. 13.

[181] Liberty. 2016. Liberty's summary of the Investigatory Powers Bill for Second Reading in the House of Commons. March 2016.

[182] *Id.*

[183] *Id.,* p. 24, paragraph 93.

[184] Malgorzata Tomkiewicz, 'Podsluchy operacyjne w orzecznictwie sadowym' [Extra-judicial eavesdropping in case law] (2015) *Prokuratura i Prawo* 4, 153-171.

Tied to this criticism is the fact that there is no representative of the target involved in the authorisation process for the use of hacking techniques.[185]

However, many elements of the Member State legal provisions, including the fact that most Member States have specific legal provisions, are in fact positive. Box 8 details selected good practice elements.

Box 8: Select good practice elements of the legislative provisions for hacking by law enforcement.

Select good practice: Member State legislative frameworks

Germany: Although they were deemed unconstitutional in a 2016 ruling, the provisions for the screening and deletion of data related to the core area of private life are a positive step. If the provisions are amended, as stipulated in the ruling, to ensure screening by an independent body, they would provide strong protection for this private data.

Italy: The 2017 draft Italian law includes a range of provisions related to the development and monitoring of the continued use of hacking tools. As such, one academic stakeholder remarked that the drafting of the law must have been driven by technicians. However, these provisions bring significant benefits to the legislative provisions in terms of supervision and oversight of the use of hacking tools. Furthermore, the Italian draft law takes great care to separate the functionalities of the hacking tools, thus protecting against the overuse or abuse of a hacking tool's extensive capabilities.

Netherlands: The Dutch Computer Crime III Bill stipulates the need to conduct a formal proportionality assessment for each hacking request, with the assistance of a dedicated Central Review Commission (*Centrale Toetsings Commissie*). Also, the law requires rules to be laid down on the authorisation and expertise of the investigation officers that are allowed to perform hacking.

4.4. Technical means used by law enforcement

This section presents the study findings on the hacking techniques used by law enforcement agencies. Based on the legislative provisions, this section will discuss how these technical means are represented in the legislation, drawing out any trends and difficulties across the six Member States examined. Furthermore, specific focus will be placed on the legislative provisions related to zero-day vulnerabilities and their practical application.

Many of the Member State legislative frameworks add specificity around the types of activities that can be undertaken and provide a better understanding of the technical means available to law enforcement, when compared with previous legislation.

For instance, the 2016 amendments to the Polish Police Act permit the following, under certain conditions: "extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems" (Article 19 §6). Before the amendment, Article 19 simply permitted the "use of technical means, which facilitate obtaining information and evidence in secret as well as recording thereof" – the interpretation of these provisions can be very broad. In fact, the Council of Europe's Venice Commission applauded these improvements in their critique of the Polish legislation.[186]

[185] Expert workshop conducted for this study.

[186] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016, p. 13.

Furthermore, the 2017 Italian draft law and the Dutch Computer Crime III Bill add significant legislative detail regarding the technical functionalities that are permitted, as detailed in Table 10.

Table 10: Additional legislative specificity regarding hacking techniques.

Italy

It is widely acknowledged that Italian law enforcement agencies use hacking techniques in the process of criminal investigations.[187] In fact, experts consider that the use of malware is the method of choice for Italy's law enforcement agencies.[188] As such, Italy's 2017 draft law aims to effectively regulate the separate functionalities of such a trojan, which would have the capability, among others, to track an individual, intercept communications at source through control over both a device's microphone and camera, access stored data, etc. This separation of functionalities allows for greater recognition of how such a tool would be used.

Furthermore, as described in previous sections, the Italian legislation presents a range of innovative provisions related to monitoring the development and use of trojans to ensure greater oversight and reduce abuse.

Netherlands

The Dutch Computer Crime III Bill states both the functionalities and the techniques that may be used by law enforcement to enter and search a computerised device. The purposes listed include:

- Undertaking an online search (stored data), including looking at the data and securing the data.
- Intercept private information (streaming data), including capturing key strokes (incl. passwords) and real-time monitoring of data traffic (which may or may not include encryption).
- Influence the data, by adjusting settings, turning on webcams / microphones, sabotaging or turning a device off.
- Deleting the data.

In terms of techniques, law enforcement agencies are permitted to:

- Use a vulnerability in the IT system;
- Enter / intrude using a false identity or by brute force.
- Use a trojan to infect the device with malware.

However, **other Member States employ broader terms** within the legislation and do not provide any specificity (either in legislative or practical terms) on the hacking tools and techniques used by law enforcement.

For example, there is very little publicly available information on the tools that UK law enforcement agencies use, as highlighted by the National Crime Agency (NCA)'s statement: "the NCA leads the law enforcement response to serious and organised criminality impacting the UK. However, to preserve operational effectiveness we do not routinely disclose details

[187] Citizen Lab. 2014. Mapping Hacking Team's "Untraceable" Spyware. Accessed on 28.02.17 at: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

[188] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

of specific tools or techniques deployed in addressing those threats."[189] As such, an academic expert remarked that this non-disclosure of information and non-specific nature of legislation regarding tools is reported to allow the law enforcement agencies to keep their options open for the use of hacking.[190]

Although Poland has improved the specificity of its legislation regarding the purpose of using hacking tools, the same specificity is not applied to the techniques in use. In fact, all techniques and methods used by law enforcement agencies are classified.

Regarding those Member States that are providing more specificity on technical capabilities, the findings suggest a clear **trend towards the development of in-house expertise** and even in-house hacking tools. Examples are presented in Table 11.

Table 11: Examples of in-house development of expertise and tools.

France
A member of the French judiciary stated that French law enforcement primarily use keyloggers to collect data through their legislative hacking provisions. Furthermore, the French authorities (through a combination of the Ministry for Justice and the Ministry of the Interior) have developed in-house tools for remote access. However, as technical investigative tools must be legally authorised, this process took time. Furthermore, once the tools were authorised, other aspects of the tools were disputed and these in-house tools have recently been reinitialised.[191] As such, these tools are not available to law enforcement but demonstrate the intention of the French authorities.
Germany
In 2011, an externally developed and acquired software was installed on a source laptop and used by law enforcement to intercept telecommunications data. However, this was criticised and determined to be unlawful because the software had the ability to turn on the laptop's camera and microphone, even though the law enforcement agency did not use this functionality.[192] Since this incident, it is reported that the BKA no longer purchases external hacking expertise but intends to develop its own tools.[193] Furthermore, the German Government does have expertise in hacking practices. The German Ministry of Interior has recently established a new authority – ZITiS – which will support German law enforcement through the provision of technical skills and expertise in these hacking practices. ZITiS will reportedly be staffed with 400 individuals.[194] Furthermore, the CCITÜ has existing capabilities in this area, as does the Federal Police and certain state criminal police forces. It is not clear how these entities will work alongside one another.
Italy
A range of legislative provisions have been included in the 2017 draft law that suggest the Italian authorities intend to develop capabilities in this area. For instance, the draft law states that trojans must be operated by in-house personnel and not private contractors.

[189] Cox, J. 2016. What the UK's Proposed Surveillance Law Means for Police Hacking. *Motherboard.*

[190] Bernal, P. 2017. Expert interview conducted for this study.

[191] Legrand, E. 2017. Expert interview conducted for this study.

[192] Franosch, R. 2017. Expert interview conducted for this study.

[193] Franosch, R. 2017. Expert interview conducted for this study.

[194] Paganini, P. 2016. ZITiS is the new German Government cyber unit formed in the wake of terror attacks. Security Affairs article. http://securityaffairs.co/wordpress/50297/terrorism/zitis-german-cyber-unit.html.

Furthermore, the source code of trojans used by law enforcement must be deposited to a specific authority and must be verifiable with a reproducible build process.

An additional point explored through the country reports is how the Member States legislate for the **use of zero-day vulnerabilities**. In fact, only one Member State makes specific reference to this mechanism for gaining access to a device.

As mentioned above, the Dutch Computer Crime III Bill permits the use of a vulnerability in the IT system to gain access. In addition, the legislation dictates that law enforcement may not purchase zero-day vulnerabilities and must report any exploited vulnerabilities to the relevant organisation. However, in practice, a Dutch NGO[195] reported that law enforcement agencies are permitted to buy commercial software that exploits known and unknown vulnerabilities and that law enforcement have previously denied the release of information on the technical means they use, based on the same argument employed by the UK's NCA.[196] This position potentially contravenes the obligation to report and not purchase zero-day vulnerabilities.

Although explicit mention is not made in the legislative provisions of other Member States, certain provisions aim to ensure that the technical security of the device is not impinged by law enforcement hacking practices. For example, the Italian draft law stipulates that a trojan shall not reduce the security level of a device and shall be removed from the target device. Similar provisions exist in Germany and France.

In **conclusion**, the legislative provisions in the Member States examined add specificity when compared with previous laws. In particular, this specificity clarifies the purpose of the use of hacking tools, although the proposed Dutch and Italian legislative acts also provide more specificity on the tools and techniques to be used. In other Member States, details on the tools and techniques are classified and not publicly available. Furthermore, a prominent trend in this area relates to the development of in-house expertise and hacking tools.

Zero-day vulnerabilities are only mentioned in the legislative provisions and practical discussions by one Member State, although provisions that aim to infer protection of device security are stipulated by other Member States. This Member State, the Netherlands, requires the reporting of exploited vulnerabilities and prohibits law enforcement from purchasing zero-day vulnerabilities.

4.5. Security and intelligence services: legal framework

This section presents the study findings on the rules and possibilities for hacking by security services and places them against those described for law enforcement, above. The intention is to discuss how the legal frameworks and practices are comparable, before evaluating if good practices can be transferred from the security and intelligence agencies to the law enforcement sphere. However, as this section does not represent the primary focus of the study, and existing research extensively covers the topic, it has not been possible to delve into as great depths within the legal frameworks for the security and intelligence services as for law enforcement.

Primarily, it is found that, when the security and intelligence services conduct targeted hacking, experts state that parallels can be drawn with law enforcement practices in terms of the types of hacking techniques used. However, **key differences exist regarding the**

[195] Siedsma, T. 2016. Bits of Freedom – Expert interview conducted for this study.

[196] https://zoek.officielebekendmakingen.nl/ah-tk-20142015-202.html.

extent of capabilities within the security and intelligence services and the scale of use. This is illustrated by the March 2017 Vault7 leak[197] profiled in Box 9, below.

Box 9: Profile of the Vault7 publication of reportedly CIA documents.

Vault7: Profile

"Year Zero" was published by WikiLeaks on 7 March 2017 and represents the first full part of the "Vault7" suite of leaked documents. According to WikiLeaks, "Vault7" contains the "largest ever publication of confidential documents on the [CIA]"[198]. "Year Zero" alone claims to comprise 8,761 documents from "an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence"[199].

WikiLeaks claims that the rationale for the release of these documents is that urgent debate is needed on whether these reported capabilities exceed the CIA's mandated powers and whether public oversight of the agency is sufficient.

Key findings:

- "Year Zero" describes the scope and direction of the CIA's global covert hacking program. This hacking program has reportedly established a 'hacking arsenal' (as termed by WikiLeaks) which includes malware, viruses, trojans, weaponised zero-day exploits and malware remote control systems. Furthermore, zero-day vulnerabilities have reportedly been 'hoarded' by the CIA;
- By the end of 2016, the CIA's hacking division had over 5,000 registered users and had produced more than 1,000 hacking systems, trojans, viruses and other 'weaponised' malware. Hacking targets include products from renowned US, EU and Asian technology companies (e.g. Apple, Nokia, Blackberry, Kaspersky, Siemens, Google, Microsoft and Samsung);
- CIA presence, and cooperation with actors, within the EU is reported: for instance, the US consulate in Frankfurt is reportedly a covert base for US hackers covering Europe, the Middle East and Africa; and the Weeping Angel attack which converts Samsung smart TVs into microphones was developed in collaboration with MI5/BTSS;
- WikiLeaks report that these documents have undergone unauthorised circulation among US government hackers and contractors prior to their release. As such, the leak, if in the hands of malicious actors, provides access to several hundred million lines of code and brings an "extreme proliferation risk" for hacking techniques, vulnerabilities and cyberwar 'weapons'.

Although not all (if any) intelligence and security agencies have the required resources to develop similar capabilities to those described above, Box 9 at least demonstrates that, in most cases, these agencies have significantly greater capabilities than are available to law enforcement. This is further supported by the national-level research conducted for this study (see examples in Table 12).

[197] WikiLeaks. 2017. Vault 7: CIA Hacking Tools Revealed.
[198] WikiLeaks. 2017. Vault 7: CIA Hacking Tools Revealed.
[199] WikiLeaks. 2017. Vault 7: CIA Hacking Tools Revealed.

Table 12: Difference in capabilities between the security and intelligence services and law enforcement.

United Kingdom

In the UK, for example, many of the same legislative conditions apply to law enforcement and security service hacking. However, the legal framework for security services permits the provision of bulk equipment interference warrants, as well as the ability to undertake these interference practices overseas. Furthermore, the process for authorisation is typically faster. These conditions provide capabilities substantially beyond the provisions included for law enforcement agencies.

As such, and as demonstrated in the documents leaked by former NSA contractor Edward Snowden, the security services have the capabilities to use implant tactics that would not be possible under the law enforcement legal provisions. For example, one technique reportedly used by UK security services is the sending of spam phishing emails that inject malware to exfiltrate files, reveal the location of a device, log browsing patterns, covertly record audio, or take snapshots through a device's camera. The Snowden documents reveal that the NSA and, inferred through shared capabilities, the UK security services can infect enough devices to create an implant network consisting of millions of devices.[200]

Poland

Similarly, Polish legislation provides for many of the same conditions across law enforcement and security service hacking. However, legislation enacted in June 2016 (the Act on anti-terrorist activities) has been heavily criticised for its wide provision of capabilities to Polish intelligence agencies. For example, the Internal Security Agency (ABW) is now permitted to undertake security evaluations, allowing them to access data from all government agencies and private companies that provide critical infrastructure services.[201] Amnesty International criticised the Act, stating that it "consolidates sweeping powers, including enhanced surveillance capacity […] with no independent oversight mechanism".[202]

In addition to the above, a 2015 report of the EU Agency for Fundamental Rights (FRA) entitled 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU'[203] mapped the legal frameworks for surveillance across the EU28 at the behest of the European Parliament. This report found that many of the legal provisions currently in place to govern the use of hacking tools by the security and intelligence services are insufficient regarding the protection of fundamental rights. Examples are presented in Table 13.

[200] Gallagher, R. & Greenwald, G. 2014. How the NSA Plans to Infect 'Millions' of Computers with Malware. *The Intercept*.

[201] Amnesty International. 2016. Poland: Counter-terrorism bill would give security service unchecked power. Public Statement. EUR 37/4263/2016.

[202] *Id.*

[203] European Union Agency for Fundamental Rights. 2015. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member States' legal frameworks.

Table 13: Key findings on Member State legal frameworks for surveillance by FRA.

Intelligence services and surveillance laws
Notion of national security
Protecting national security is the primary aim of EU security and intelligence services. However, this notion is rarely defined and is referred to differently across EU Member States.
Legal regulation of surveillance
The line between the tasks of law enforcement and the intelligence service is sometimes blurred. Furthermore, most Member State legal frameworks regulate targeted surveillance but lack clear and applicable definitions of human rights standards.
Oversight of intelligence services
Executive control and coordination between oversight bodies
Diversity of Member State legal and political systems has translated into a great variety of bodies that oversee the intelligence services. As such, EU Member States present vastly different oversight systems where "a great assortment of powers are granted to the various oversight bodies".
Parliamentary oversight
24 EU Member States provide for parliamentary oversight of security service activities, although no parliamentary committee is granted unrestricted access to intelligence information.
Expert oversight
15 Member States complement the work of parliamentary oversight mechanisms with expert bodies dedicated to intelligence service oversight. In some Member States, however, the authorisation of surveillance measures does not involve any institutions that are independent of the intelligence services.
Remedies
Obligation to inform and the right to access
All Member States place restrictions on the obligation to inform and the right to access information; in fact, eight do not have any legislative provisions at all on the matter. In 10 Member States, oversight bodies review restrictions on these rights.
Judicial remedies
All Member States provide the opportunity to complain about privacy violations via the courts. However, the lack of specific relevant knowledge within the judiciary limits this right to effective remedy.
Non-judicial remedies
In most Member States, the relevant oversight bodies for non-judicial remedies are independent institutions. Elements that can facilitate access to remedies include more relaxed rules on the evidentiary burden and class actions, as well as effective protection of whistle-blowers.

In combination with the above findings on the extent of capabilities and scale of use, this suggests that the legal frameworks and practices used by security and intelligence services should not be held up as an example of good practice to law enforcement agencies. However, the release of Vault7, as was the case for the Snowden revelations, will likely result in significant debate on the topic at international and EU fora. One potential good practice is the appropriation of this scrutiny to the use of hacking techniques by law enforcement.

5. CONCLUSIONS

The use of hacking techniques by law enforcement agencies evolved organically to solve the challenge of 'Going Dark'. "Going Dark is a term used by law enforcement agencies to describe their decreasing ability to lawfully access and examine evidence at rest on devices and evidence in motion across communications networks."[204] A significant barrier to this access is encryption. Thus, the argument follows that lack of access to such evidence places public safety at risk and will, to a certain extent, result in impunity. Overcoming this barrier resulted in law enforcement use of hacking techniques to bypass encryption technologies.

Despite the investigative benefits of increased data access, law enforcement hacking also presents several significant risks. Primarily, police hacking risks significantly impacting the fundamental right to privacy. Furthermore, it may have potential implications for the security of the internet and, to a lesser extent, territorial sovereignty. These risks are detailed in Table 14.

Table 14: Risks presented by law enforcement use of hacking techniques.

Risk to the fundamental right to privacy
Hacking techniques are extremely invasive, particularly when compared with traditionally invasive investigative tools (e.g. wiretapping). Thus, their use is **inherently in opposition to international, EU and national-level legislation protecting the fundamental right to privacy.** As detailed in both the Charter of Fundamental Rights of the EU (Article 7) and the European Convention on Human Rights (Article 8), this restriction is lawful only if it is: • Provided for by law; • Subject to the principles of proportionality; and • Necessary. This risk has been extensively discussed at international and EU-level fora, although in most cases within wider discussions related to surveillance practices. As such, recommendations from these fora provide a baseline against which to judge the specific provisions stipulated in Member State legal frameworks.
Risk to the security of the internet
Hacking techniques, by their very nature, use vulnerabilities to gain access to an IT system. As such, the **discovery and exploitation of such vulnerabilities presents risks to the security and functioning of the hacked system and the wider internet**. A specific example, and the primary focus of debates on the topic, is the discovery and exploitation of zero-day vulnerabilities by law enforcement agencies. Civil society actors argue that, if discovered, governments should immediately report zero-day vulnerabilities at risk of undermining the security of the internet, given the potential damage that can be done if such a vulnerability is discovered by a malicious actor.
Risk to territorial sovereignty
Given the nature of the internet, the expansion of cloud computing services and the fact that these services and channels are owned and controlled by private international companies,

[204] IACP Summit Report. 2015. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence.

many services are provided across borders. Therefore, the target data of a law enforcement hack may be located anywhere in the world.

This 'loss of knowledge of location' means that, when conducting investigations using hacking techniques, **law enforcement agencies risk extraterritorial hacking and breaching the international legal principle of sovereignty**.

Given the scale of these risks, significant debate would be expected at international and EU fora on the use of hacking by national-level law enforcement agencies. In fact, there have been no discussions focused specifically on this topic. The discussions that have addressed this topic to some extent have primarily focused on the surveillance activities of the security and intelligence services. As discussed below, the specific legal conditions and mechanisms governing law enforcement hacking at Member State level strongly reflect the related international-level findings and recommendations for surveillance activities.

Furthermore, these international-level discussions start from a point of view where surveillance activities are necessary and simply require governing laws. This aspect seems to have transferred into law enforcement hacking, with all stakeholder discussions starting from a position where such hacking is deemed necessary.

However, the use of hacking techniques and the implementation of specific legislation at the national level **should be subject to EU and international fundamental rights principles**. As such, prior to the use and legislation of such techniques, an informed decision should be taken on the necessity of law enforcement hacking capabilities on the basis of national context, the particular challenges facing national police forces and the abovementioned risks. It is thus concluded that **the right for law enforcement agencies to use hacking techniques should not be assumed but must be deemed necessary within the specific context of a Member State**.

Regarding the Member States examined for this study, however, law enforcement hacking practices are seemingly necessary. All Member States have adopted or are in the process of adopting specific legislation on the topic. Furthermore, for most Member States, the development of specific legislative provisions has only begun recently.

As such, law enforcement agencies in all Member States have used, or still use, hacking techniques, prior to the introduction of specific legislative provisions, under so-called 'grey area' legal provisions (i.e. provisions not intended to govern the use of hacking techniques). Given the potential invasiveness of hacking techniques, these **'grey area' provisions are considered insufficient to adequately protect the right to privacy.**

Where specific legal provisions have been adopted, all stakeholders agree that a restriction of the right to privacy requires the implementation of certain safeguards. As discussed at length in section 4.2, in their current or proposed law the six Member States examined all have a suite of *ex-ante* conditions and *ex-post* mechanisms that aim to ensure that the use of hacking techniques is proportionate and necessary. As recommended by various UN bodies, the provisions of primary importance include judicial authorisation of hacking practices, safeguards related to the nature, scope and duration of possible measures (e.g. limitations to crimes of a certain gravity, only for a certain duration, etc.) and independent oversight.

Although certain elements can be called good practices, they are only aspects of what needs to be a comprehensive suite of conditions and mechanisms safeguarding the fundamental right to privacy. As such, substantial criticisms have been levied across the six Member States, with no Member State devoid of criticism.

With these criticisms in mind, it is concluded that the **specific national-level legal provisions examined provide for the use of hacking techniques in a wide array of circumstances**. The varied combinations of requirements, including those related to the gravity of crimes, the duration and purpose of operations and the oversight, result in a situation where the law does not provide for much stricter conditions than are necessary for less intrusive investigative activities such as interception.

Furthermore, in addition to the legislative text, there **will always be the need for discretion in the practical application of legal provisions for such invasive investigative tools**.

The conclusions related to the presence of fundamental rights safeguards in the specific Member State laws are also relevant given that limiting law enforcement's use of hacking techniques will also reduce the risk to the security of the internet. Furthermore, some Member States include specific provisions mitigating this risk, including tracking the development and use of hacking tools and ensuring the complete removal of hacking tools from the target device after use. However, such provisions are not present in all Member States.

6. RECOMMENDATIONS AND POLICY PROPOSALS

Based on the study findings, relevant and actionable **policy proposals and recommendations** have been developed under the two key elements: i) the fundamental right to privacy; and ii) the security of the internet.

Recommendations and policy proposals: Fundamental right to privacy

It is recommended that the use of 'grey area' legal provisions is not sufficient to protect the fundamental right to privacy. This is primarily because existing legal provisions do not provide for the more invasive nature of hacking techniques and do not provide for the legislative precision and clarity as required under the Charter and the ECHR.

Furthermore, many of these provisions have only recently been enacted. As such, there is a need for robust evidence-based monitoring and evaluation of the practical application of these provisions. It is therefore recommended that the application of these new legal provisions is evaluated regularly at national level, and that the results of these evaluations are assessed at EU-level.

If specific legislative provisions are deemed necessary, the study recommends a range of good practice, specific *ex-ante* and *ex-post* provisions governing the use of hacking practices by law enforcement agencies, including:

- Ensure the scope of the use of hacking techniques is appropriately minimised regarding the gravity of crimes and the duration of the order;
- Ensure that hacking techniques must be targeted and that bulk or untargeted use of hacking not be permitted;
- Ensure legislative separation of functionalities of a hacking tool and authorisation for use of those functionalities;
- Ensure appropriate steps are taken to effectively monitor the development and use of hacking tools;
- Ensure provisions are implemented to ensure the data collected are minimised to the greatest extent possible;
- Ensure effective challenge of requests to use hacking techniques at the authorisation phase. As it is not possible for the target of such a request to challenge a hacking order, this process could benefit from the engagement of independent stakeholders with fundamental rights and technical expertise; and
- The authorisation phase could be further supported by specific legislative references and formal tests related to the information to be included in authorisation requests and the assessments of proportionality and necessity.

Furthermore, more focus should be placed on the provisions governing the handling and storage of data during an investigation.

Regarding *ex-post* mechanisms for supervision and oversight, further guidance is required on what provisions may be appropriate for Member States to implement. Discussions at international fora have primarily focused on *ex-ante* conditions, with limited focus given to *ex-post* mechanisms.

One practice, that is common in Member State legislation related to security service surveillance but less common regarding law enforcement hacking techniques, is the presence and role of a parliamentary oversight committee. These committees should have access to both macro and micro-level data on the use of hacking techniques by law enforcement. Furthermore, public reporting of data on these practices should be introduced in more Member States, thereby improving the transparency of such practices, and the input of national-level data protection authorities should be sought on these matters.

Policy proposal 1: *The European Parliament should pass a resolution calling on Member States to conduct a Privacy Impact Assessment when new laws are proposed to permit and govern the use of hacking techniques by law enforcement agencies. This Privacy Impact Assessment should focus on the necessity and proportionality of the use of hacking tools.*

Policy proposal 2: *The European Parliament should reaffirm the need for Member States to adopt a clear and precise legal basis if law enforcement agencies are to use hacking techniques.*

Policy proposal 3*: The European Parliament should commission more research or encourage the European Commission or other bodies to conduct more research on the topic. In response to the Snowden revelations, the European Parliament called on the EU Agency for Fundamental Rights (FRA) to thoroughly research fundamental rights protection in the context of surveillance. A similar brief related to the legal frameworks governing the use of hacking techniques by law enforcement across all EU Member States would act as an invaluable piece of research.*

Policy proposal 4: *The European Parliament should encourage Member States to undertake evaluation and monitoring activities on the practical application of the new legislative provisions that permit hacking by law enforcement agencies.*

Policy proposal 5: *The European Parliament should call on the EU Agency for Fundamental Rights (FRA) to develop a practitioner handbook related to the governing of hacking by law enforcement. This handbook should be intended for lawyers, judges, prosecutors, law enforcement officers and others working with national authorities, as well as non-governmental organisations and other bodies confronted with legal questions in the areas set out by the handbook. These areas should cover the invasive nature of hacking techniques and relevant safeguards as per international and EU law and case law, as well as appropriate mechanisms for supervision and oversight.*

Policy proposal 6: *The European Parliament should call on EU bodies, such as the FRA, CEPOL and Eurojust, to provide training for national-level members of the judiciary, in collaboration with the abovementioned handbook, on the technical means for hacking in use across the Member States, their potential for invasiveness and the principles of necessity and proportionality in relation to these technical means.*

Recommendations and policy proposals: Security of the internet

The primary recommendation related to the security of the internet is that the position of the EU against the implementation of 'backdoors' and in support of strong encryption standards should be reaffirmed, given the prominent role encryption plays in our society and its importance to the EU's Digital Agenda. To support this position, the EU should ensure continued engagement with global experts in computer science as well as civil society privacy and digital rights groups.

The actual impacts of hacking by law enforcement on the security of the internet are yet unknown. More work should be done at the Member State level to assess the potential impacts such that these data can feed in to overarching discussions on the necessity and proportionality of law enforcement hacking. Furthermore, more work should be done, beyond understanding the risks to the security of the internet, to educate those involved in the authorisation and use of hacking techniques by law enforcement.

At present, the steps taken to safeguard the security of the internet against the potential risks of hacking are not widespread. As such, the specific legislative provisions governing the use of hacking techniques by law enforcement, if deemed necessary, should safeguard the security of the internet and the security of the device, including reporting the vulnerabilities

used to gain access to a device to the appropriate technology vendor or service provider; and ensure the full removal of the software or hardware from the targeted device.

Policy proposal 7: *The European Parliament should pass a resolution calling on Member States to conduct an Impact Assessment to examine the impact of new or existing laws governing the use of hacking techniques by law enforcement on the security of the internet.*

Policy proposal 8: *The European Parliament, through enhanced cooperation with Europol and the European Union Agency for Network and Information Security (ENISA), should reaffirm its commitment to strong encryption considering discussions on the topic of hacking by law enforcement. In addition, the Parliament should reaffirm its opposition to the implementation of 'backdoors' in information technology infrastructures or services.*

Policy proposal 9: *Given the lack of discussion around handling zero-day vulnerabilities, the European Parliament should support the efforts made under the* cybersecurity contractual Public-Private Partnership (PPP) *to develop appropriate responses to handling zero-day vulnerabilities, taking into consideration the risks related to fundamental rights and the security of the internet.*

Policy proposal 10: *Extending policy proposal 4, above, the proposed FRA handbook should also cover the risks posed to the security of the internet by using hacking techniques.*

Policy proposal 11: *Extending policy proposal 5, training provided to the judiciary by EU bodies such as FRA, CEPOL and Eurojust should also educate these individuals on the risks posed to the security of the internet by hacking techniques.*

Policy proposal 12: *Given the lack of discussion around the risks posed to the security of the internet by hacking practices, the European Parliament should encourage debates at the appropriate fora specific to understanding this risk and the approaches to managing this risk. It is encouraged that law enforcement representatives should be present within such discussions.*

APPENDIX 1: EU COUNTRY REPORTS

France Country Report

Completed with the support of Emmanuelle Legrand, investigating judge with specific expertise in cybercrime.

Legal framework and context

The French authorities have prominently stated on several occasions that encryption is a significant challenge to law enforcement agencies. For example, in August 2015, the Paris chief prosecutor, in collaboration with the commissioner of the City of London Police, the chief prosecutor of the High Court of Spain and the Manhattan district attorney, penned an op-ed for the *New York Times* entitled 'When Phone Encryption Blocks Justice'.[205] This article argues that the increasing prevalence of full-disk encryption on mobile phones results in impunity and, at the minimum, hinders investigations.[206]

A year later, French Minister of the Interior, Bernard Cazeneuve, in collaboration with his German counterpart, Thomas de Maizière, continued this trend.[207] Although Cazeneuve made mention of the important role encryption plays in society, he also noted the increasing challenge encryption poses to law enforcement agencies and called for better ways for law enforcement to access encrypted communications, particularly those sent via messaging applications with end-to-end encryption. These comments received widespread criticism from civil society.[208,209,210] The subsequent debates covered the seemingly contradictory nature of the statements; the related human rights considerations; and the influence of terrorism on the declaration.

As discussed throughout this study, techniques borrowed from the hacking community are increasingly being used by law enforcement to access data pertinent to investigations, often through the circumvention of security measures such as encryption. Subsequently, many Member States, including France, have implemented, or appropriated, specific legal provisions to ensure that the use of such techniques is lawful and balanced with respect to the fundamental rights. However, the above statement by the French and German Ministers suggests the preferred strategy is ensuring that ICT vendors provide access to decrypted data.[211] As such, many commentators have remarked that this is akin to the introduction of 'backdoors' and all the related criticisms (see chapter 2 for more information).[212]

---

[205] Vance, C. Y., Molins, F., Leppard, A. and Zaragoza, J. 2015. When Phone Encryption Blocks Justice. The Opinion Pages. The New York Times, August 11, 2015.

[206] *Id.*

[207] Franco-German initiative on internal security in Europe, Joint statement by the French and German Ministers of the Interior. 23 August 2016, Paris. Accessed in FR on 24.01.17 at: http://www.interieur.gouv.fr/Archives/Archives-ministre-de-l-interieur/Archives-Bernard-Cazeneuve-avril-2014-decembre-2016/Interventions-du-ministre/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe.

[208] Järvinen, H. 2016. France and Germany: Fighting terrorism by weakening encryption. Article for EDRi. Accessed on 02.03.17 at: https://edri.org/france-germany-fighting-terrorism-by-weakening-encryption/.

[209] Lomas, N. 2016. Encryption under fire in Europe as France and Germany call for decrypt law. Article for TechCrunch. Accessed on 02.03.17 at: https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/.

[210] Griffin. A. 2016. WhatsApp privacy under threat as France and Germany push EU to allow states to break encryption. Article for *The Independent*. Accessed on 02.03.17 at: http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-privacy-under-threat-as-france-and-germany-push-eu-to-allow-states-to-break-encryption-a7204961.html.

[211] Reuters. 2016. France, Germany press for access to encrypted messages after attacks.

[212] Statewatch. 2016. German and French Interior ministers demand EU discussion on undermining encryption. Accessed on 02.03.17 at: http://statewatch.org/news/2016/nov/de-fr-comms-letter.htm.

In the context of the use of hacking tools and techniques, therefore, it is not surprising that an investigative judge remarked that, although the legal possibilities exist, French judges and prosecutors do not have the requisite knowledge to use such tools.[213] Furthermore, those with the insight to apply these technical tools do not have access to such tools – the reasons for which will be discussed below.[214] Therefore, this investigative judge noted that hacking tools are not that widely used in France.

However, legal provisions governing the use of hacking tools do exist within the French Code of Criminal Procedure (*Code de procédure pénale*), and provisions on the interception of electronic correspondence by the security services are also included in state security law, which governs the prevention of terrorism, organised crime and organised delinquency.[215] These topics will be discussed in greater detail below.

Although there is no constitutional right to privacy or confidentiality of communications in France, the right to privacy is provided for in Article 9 of the *Code Civil* as well as the Post and Electronic Communications Code (*Code des postes et des communications électroniques*) and the domestic law application of the European Convention on Human Rights.[216] Furthermore, the right to privacy has been embodied in several decisions of the Constitutional Court.[217]

Provisions of the legal framework – *ex-ante* considerations

The legal provisions for the use of hacking tools by law enforcement is solely governed by the French Code of Criminal Procedure and, more specifically, the amendments of LOI n° 2016-731 of 3 June 2016 strengthening the fight against organised crime, terrorism and their financing.[218]

LOI n° 2016-731 amended section 6 of Chapter II of Title XXV of Book IV and provides for two legal possibilities: i) remote access initiated by the physical installation of software on a target computer; and ii) remote access to computerised data, initiated remotely.[219] Both possibilities are covered by Articles 706-102-1 and 706-102-2. The difference between these articles relates to authorisation: in 706-102-1, the public prosecutor is required to gain authorisation from the judge of freedoms and detention (*le juge des libertés et de la détention*); whereas 706-102-2 relates to the investigating judge who, as an independent judge, is permitted to authorise the use of these possibilities.

Further *ex-ante* conditions apply to these possibilities. The use of such techniques is only permissible for offences falling within the scope of Articles 706-73 and 706-73-1.[220] These articles provide a list of crimes covering serious and organised crime and terrorism, although there is only one reference to cybercrime.

---

[213] Legrand, E. 2017. Expert interview conducted for this study.

[214] Legrand, E. 2017. Expert interview conducted for this study.

[215] Sieber, U. and von zur Mühlen. 2016. Access to Telecommunication Data in Criminal Justice: A Comparative Analysis of European Legal Orders. Duncker & Humblot, Berlin, pp. 441-442.

[216] Korff, D., Wagner, B., Powles, J., Avila, R. and Bürmeyer, U. (2017) Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes. Global Report – January 2017. Available at SSRN: https://ssrn.com/abstract=2894490

[217] see Decision no. 2009-580 DC of 10 June 2009; Decision no. 94-352 DC of 18 January 1995; Decision no. 99-422 DC of 9.11.1999; Decision no. 99-419 DC of 9.11.1999; Decision no. 99-416 DC of 23.07.1999; Françoise MONÉGER - Nouveaux Cahiers du Conseil constitutionnel n° 39 (Dossier : la Constitution et le droit des personnes et de la famille) - avril 2013.

[218] LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale (1). Accessed on 03.03.17 at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231&categorieLien=id

[219] Code de procédure pénale, articles 706-102-1 and 706-102-2.

[220] Code de procédure pénale, articles 706-73 and 706-73-1.

Furthermore, the legislative amendments provide for the following *ex-ante* considerations:[221]

- **Article 706-102-3** states the information that should be provided in a request for the use of hacking techniques. Such a request should stipulate the offence that motivates the use of such techniques, the exact location or detailed description of the device to be accessed and the duration for which such techniques will be used.

  This article goes on to state that judicial authorisation for operations under Article 706-102-1 can be issued for a maximum period of one month, renewable once under the same conditions. Authorisations under Article 706-102-2 are permitted for a longer duration, up to a maximum initial period of four months, renewable under the same conditions up to a total of two years. As discussed above, this difference relates to the different authorisations required.
- **Article 706-102-4** states that the operations shall be carried out under the authority and control of the authorising judge, who may at any point order the interruption of such operations. Furthermore, the aims of the operation may not extend beyond investigating and confirming the offences stated in the authorisation decision.
- **Article 706-102-5** provides protection for certain professions or professional groups that are required to ensure confidentiality; for example lawyers, journalists and doctors.

Additional provisions in the Code of Criminal Procedure relate to ensuring access to protected data on devices already seized. For such cases, **Articles 230-1** and **230-2**[222] stipulate that the public prosecutor or the investigating judge may request the services of a qualified individual or the Centre for Technical Assistance,[223] a classified organisation, to access the data.

One investigative challenge noted by an investigating judge relates to ensuring the chain of custody of the data collected through the means described above. At present, there are no legal provisions related to this challenge, and no uniformity in practice across law enforcement agencies. There are simply general principles to follow on ensuring the integrity of evidence.[224]

Furthermore, once access has been obtained using hacking tools, the Code of Criminal Procedure also governs the safeguards related to the collection and use of data (e.g. intercepting communications, copying stored data, handling collected data, etc.). Key provisions in this regard include section 3 of Chapter I of Title III of Book I (Articles 92 to 100-7), which concerns the inspections of premises, searches, seizures and interception of correspondence by telecommunications[225]; Article 56, which relates to the seizure and recording procedures for the handling of seized computer data; and Article 60-3, which permits the employment of technical experts by the prosecutor to exploit protected data without impairing its integrity. Similar provisions exist in Article 156 for use by investigating judges.

Provisions of the legal framework – *ex-post* considerations

In addition to the abovementioned *ex-ante* considerations, the French legislation also includes several *ex-post* conditions for oversight and supervision of such hacking practices.

[221] Code de procédure pénale, articles 706-102-3 to 706-102-8.
[222] Code de procédure pénale, articles 230-1, 230-2.
[223] Legrand, E. 2017. Expert interview conducted for this study.
[224] Legrand, E. 2017. Expert interview conducted for this study.
[225] Code de procédure pénale, articles 92 to 100-7. Unofficial translation by John Rason Spencer QC, Professor of Law at the University of Cambridge, accessed on 03.03.17 at: http://www.legislationline.org/documents/section/criminal-codes/country/30.

As for the provisions above, these are primarily contained with section 6 of Chapter II of Title XXV of Book IV of the Code of Criminal Procedure.

- **Article 706-102-7** stipulates that, in setting up such a technical device to remotely capture data from a computer or other device, the examining magistrate or a commissioned judicial police officer shall author a report on each operation undertaken, including the date and time at which the operation began and the date on which it was completed. The aims of Article 706-102-7 are further supported by provisions stipulated in relation to electronic data in Articles 56 and 60. These articles refer to Article 163 and 166, which contain general provisions on the use of technical experts to provide access to protected evidence. Article 163 ensures a court inventory of the electronic evidence to be exploited by technical experts. Furthermore, Article 166 states that experts conducting such exploitation operations shall author a report which contains a description of the operations and their conclusions. Both the inventory and the reports shall be provided to the court and recorded via the '*procès-verbal*'.
- **Article 706-102-8** states that the investigating judge or the duly authorised judicial police officer shall record the collected data which are relevant to finding out the truth. It further stipulates that data not related to crimes stated in the authorisation order must not be kept in the record of the proceedings.
- **Article 706-102-9** stipulates that recordings of computer data shall be destroyed at the expiry of the limitation of the prosecution period and a record of such destruction shall be kept.

Fundamental rights considerations

The abovementioned conditions provide for many of the relevant and expected fundamental rights safeguards. These conditions include: limiting the use of hacking tools to criminal investigations related to a specific list of serious and organised crimes; limiting the duration of an operation; the inclusion of certain data within an application for the use of such hacking measures, including the offence, the location or description of the device and the duration of the measures; the protection provided to certain 'confidentiality' professions; the separation of authorisation for different operational functions; and the recording and reporting of these operations.

Furthermore, the '*article préliminaire*' of the Code of Criminal Procedure notes that coercive measures, such as the operations described above, are to be conducted under the effective control of the judicial authority and must be "strictly limited to the needs of the process, proportionate to the gravity of the offence charged and not such as to infringe human dignity".[226]

However, a French investigating judge noted that, due to the classified nature of the Centre for Technical Assistance, no information on the techniques, methods or tools used to access data is released or provided to the investigating judge or the court. This hinders the ability to challenge evidence resulting from such operations, as well as the ability to obtain effective remedy. Although such actions must be deemed necessary to the investigation, low limits are in place regarding the offences for which such activities are permitted. The use of the Centre for Technical Assistance is permitted for offences where the sentence may result in two or more years' imprisonment.[227]

[226] Code de procédure pénale, Article préliminaire. Unofficial translation by John Rason Spencer QC, Professor of Law at the University of Cambridge, accessed on 03.03.17 at: http://www.legislationline.org/documents/section/criminal-codes/country/30.

[227] Legrand, E. 2017. Expert interview conducted for this study.

Technical means used for hacking by law enforcement

As reported by an investigating judge, the use of keyloggers is the primary measure in use and is governed under the provisions described above. The same judge remarked that the French authorities (through a combination of the Ministry for Justice and the Ministry of the Interior) are developing the tools for remote access. However, as technical investigative tools must be legally authorised, this process took time. Since its legal authorisation, however, different opinions have been defined within the relevant authorities on these tools and these in-house tools have since been reinitialised. As such, public prosecutors and investigating judges do not have the technical means to conduct the operations set out above (i.e. Article 706-102-1 and 706-102-2).[228]

Hacking practices by the security services

France currently has three key intelligence agencies. These are The Directorate General of Interior Security (*Direction générale de la sécurité intérieure* – DGSI), which encompasses civil internal security; the Directorate General of External Security (*Direction générale de la sécurité extérieure* – DGSE), which covers civil external security; and the Directorate of Military Intelligence (*Direction du renseignement militaire* – DRM)[229].

The surveillance powers, and thus hacking practices, of these intelligence agencies are primarily governed by loi nº 2015-912 of 24 July 2015, introduced in response to several terrorist attacks and on the basis of an impact study (*étude d'impact*). This law aims to provide "a single legal framework for its intelligence gathering activities, by defining applicable principles, defining the different techniques that are used and by reinforcing control"[230].

As such, the law limits the purposes for which hacking techniques can be operationalised and states that they must only be performed with respect to the principles of proportionality.[231] Furthermore, it outlines a range of additional conditions that must be met, similar to the case of law enforcement, (e.g. related to duration, severity of the threat, prime ministerial authorisation etc.) and oversight mechanisms to ensure transparency and accountability (e.g. the Commission for Oversight of Intelligence Gathering Techniques – CNCTR, effective judicial recourse etc.).

However, several criticisms have been levied at the French intelligence law. For instance, the European Parliament noted its concern that the French law extends the capabilities of intelligence bodies and "raises important legal questions"[232]. Furthermore, the French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés* – CNIL) issued an opinion on the law, stating that it allows for broader and more intrusive surveillance measures[233].

[228] Legrand, E. 2017. Expert interview conducted for this study.

[229] European Union Agency for Fundamental Rights. 2015. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member States' legal frameworks.

[230] Dambrine, B. 2015. The State of French Surveillance Law. Future of Privacy White Paper. 22 December 2015.

[231] Law no 2015-912 of 24 July 2015 related to intelligence – Exposé des motifs.

[232] European Parliament. 2015. Follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens. P8_TA(2015)0388.

[233] Opinion no2015-078 of 5 March 2015 on intelligence bill (Délibération no2015-078 du 5 mars 2015 portant avis sur un projet de loi relative au renseignement.

Germany Country Report

Completed with the support of Dr Sven Herpig, Project Director, Transatlantic Cyber Forum, Stiftung Neue Verantwortung; and Rainer Franosch, Senior Public Prosecutor, State of Hesse.

Legal framework and context

Since 1949, the **right to privacy of correspondence, posts and telecommunications has been highly protected**, as evidenced by its prominent placement at the forefront of the German Constitution (Basic Law – *Grundgesetz* §10).[234]

Building on this longstanding respect for privacy, 2008 saw a landmark ruling in the **Federal Constitutional Court (Decision BvR 370/07)**.[235] This decision tackled what the court reported to be the first open instance of "secret access to information technology systems" – as stipulated in §5.2 no.11 sentence 1 alternative 2 of the Constitution Protection Act of the Länder of North Rhine-Westphalia (i.e. the defendant in this case).[236] The phrase "secret access to information technology systems"[237] is further explained in the ruling as "technical infiltration which for instance takes advantage of the security loopholes of the target system [i.e. system vulnerabilities], or which is effected by installing a spy program".[238] Wider debates on this topic in Germany otherwise refer to this secret access as 'online search/online surveillance' and generally discuss the intelligence community; this is discussed below.[239]

Decision BvR 370/07 declared this "secret access" null and void as it was determined to be incompatible with Art. 2.1 in conjunction with Art. 1.1, 10.1 and 19.1 of the Basic Law.[240] The decision resulted in an evolved interpretation of the right to personality[241] that encompasses the "**fundamental right to the guarantee of the confidentiality and integrity of information technology systems**".[242] Measures which merely serve to access communications, as long as they are legally and technically restricted to that purpose, are not covered by this fundamental right, but should only be measured against Art. 10 GG protecting correspondence, post and telecommunications.[243]

Decision 51, 211 of the Federal Court of Justice in Criminal Cases (*Entscheidungen des Bundesgerichtshofes in Strafsachen – BGHSt*) further contributed to this ruling. This decision stipulated that the Code of Criminal Procedure (*Strafprozessordnung – StPO*) did not currently contain a legal basis for such "secret search".[244]

German Government **policy measures complement these highly protected fundamental rights and support the protection of information systems against privacy crimes** – these measures primarily lend strong support to cryptography and its applications in encryption. Firstly, the 1999 German Government policy on cryptography –

---

[234] Art. 10 GG (German Basic Law – Grundgesetz).

[235] BVerfG, Judgment of the First Senate of 27 February 2008 – 1 BvR 370/07 – paras. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html .

[236] Art. 5.2, nr.11, sentence 1, alternative 2 VSG NRW (Constitution Protection Act – North Rhine-Westphalia).

[237] *Id.*

[238] BVerfG, Judgment of the First Senate of 27 February 2008 – 1 BvR 370/07 – paras. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html.

[239] *Id.*

[240] Art. 1.1, 2.1, 10.1 & 19.1 GG.

[241] Right to personality – Enshrined in Basic Law Article 2.1 in conjunction with Article 1.1 GG.

[242] BVerfG, Judgment of the First Senate of 27 February 2008 – 1 BvR 370/07 – paras. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html.

[243] BVerfG, Judgment of the First Senate of 27 February 2008 – 1 BvR 370/07 – paras. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html.

[244] Decisions of the Federal Court of Justice in Criminal Cases (*Entscheidungen des Bundesgerichtshofes in Strafsachen* – BGHSt) 51, 211.

which is regularly reaffirmed[245] – states the Government's intention not to legally restrict or regulate cryptographic products and procedures.[246] Secondly, an outcome of the 2015 German IT Summit – a working group that brings together Government, academia, civil society and private sector experts – was the Charter supporting End-to-End Encryption.[247] Thirdly, the Government's Digital Agenda states that "the use of encryption and other security mechanisms is necessary to ensuring Internet safety"[248] before stating the administration's aim of becoming the "world's leading country"[249] in encryption.

In addition to these significant legal and policy commitments, a joint statement by the German and French Interior Ministers in August 2016 made mention of the important role encryption plays in our society.[250] However, the key reason this statement discussed encryption was: i) to earmark the increasing challenge encryption poses to the ability of law enforcement agencies to gather investigative data; and ii) to call for better ways for law enforcement to access encrypted communications, particularly those sent via messaging applications with end-to-end encryption.[251]

With this in mind, it is found that the above jurisprudence and political commitments do not restrict the technical opportunities for hacking by law enforcement. As will be further detailed below, **hacking practices are used by law enforcement under two legal bases:** i) based on the StPO, to facilitate the interception of communications (section 100a) and the circumvention of the security of an information system that has previously been seized through due lawful procedure (section 94 and section 98); and ii) based on the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz* – BKAG), to covertly access information systems (section 20k).

Furthermore, German Government agencies are involved in these practices. In recent years, the Competence Centre for Information Technological Surveillance (CCITÜ), housed within the Federal Office of Criminal Investigation, has been the key law enforcement stakeholder in this domain; for example, CCITÜ is reported to have led the development of the German Government's trojan horse which culminated in the 2009 legal debate.[252] However, the Ministry of Interior have signalled their intent to develop the in-house skills and expertise required for these practices within a new entity – the Central Office for Information in the Security Sphere (*Zentrale Stelle für Informationstechnik im Sicherheitsbereich* – ZITiS). ZITiS will research and develop tools, but also acquire tools from vendors, and conduct training for law enforcement agencies on how to use the hardware and software. It will be focused on: telecommunication surveillance, digital forensics, cryptanalysis, analysis of bulk collected data and, in general, fighting crime, espionage etc. in the cyber realm.[253]

---

[245] Herpig, S. 2017. Expert interview conducted for this study.

[246] Principles of German Crypto Policy, Federal Cabinet of the German Government. Bonn, June 2 1999.

[247] Herpig, S. 2017. Expert interview conducted for this study.

[248] Digital Agenda 2014-2017, German Federal Government. Accessed in EN on 24.01.17 at: https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf?__blob=publicationFile&v=6.

[249] *Id.*

[250] Franco-German initiative on internal security in Europe, Joint statement by the French and German Ministers of the Interior. 23 August 2016, Paris. Accessed in FR on 24.01.17 at: http://www.interieur.gouv.fr/Archives/Archives-ministre-de-l-interieur/Archives-Bernard-Cazeneuve-avril-2014-decembre-2016/Interventions-du-ministre/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe.

[251] Franco-German initiative on internal security in Europe, Joint statement by the French and German Ministers of the Interior. 23 August 2016, Paris.

[252] Herpig, S. 2017. Expert interview conducted for this study.

[253] https://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/01/zitis-vorstellung.html.

Provisions of the legal framework – *ex-ante* considerations

As mentioned above, there are two relevant legal bases by which German law enforcement agencies can initiate hacking practices:

i. As an 'annex competence' under the **Code of Criminal Procedure – StPO.** The interception of telecommunications is well documented through section 100a *et seq.* of the StPO. Hacking by law enforcement is permitted as an 'annex competence' to these provisions – established through the German legal system's jurisprudence[254]. In this instance, such hacking facilitates this interception of telecommunications. For example, the 'annex competence' allows law enforcement the ability to access the communication before it is encrypted or after it is decrypted (e.g. by installing relevant software on the source device). Hacking is also permitted following the physical seizure of an IT product. Law enforcement agencies are legally allowed to use any means necessary to access encrypted data on a seized laptop computer. As above, this 'annex competence' is established through jurisprudence.

ii. Explicitly stated in the **Federal Criminal Police Office Act – BKAG**. Section 20k of the BKAG allows the Federal Criminal Police Office to collect data pertinent to a case through intervening with technical means in information technology systems.

Although the StPO does not contain specific provisions for the use of the abovementioned practices, both the interception of communications (integral to i) and the seizure of objects (integral to ii) require that law enforcement agencies meet a range of *ex-ante* conditions to ensure practices are lawful, taking fundamental rights into account, and that data collected are admissible as evidence in court.[255] The provisions stipulated in section 20k of the BKAG also detail a range of conditions.[256] These conditions are discussed below.

In all cases (i.e. StPO and BKAG provisions), **authorisation from the court is required**. In the StPO, there are additional provisions for exigent circumstances; it is possible for the public prosecutor's office to issue such an order but this must be confirmed by the court within three days.[257] If it is not confirmed, it becomes ineffective. Furthermore, a range of conditions need to be met for this court confirmation to be granted.

In such cases, the following conditions are required[258]:

- Suspicion of an individual based on certain facts. In the StPO, the fact that an individual has committed a serious criminal offence is required (§100a). In the BKAG, there must be danger to a person's life/freedom or national security (§20k). A list of offences considered serious, and relevant regarding intercept orders is given in StPO §100a (2). §100a (3) stipulates that such an intercept order must be targeted only against the suspect or against persons whom it can be assumed are communicating with the suspect.
- Intercepted data concerning the core area of the private conduct of life is regarded as off-limits and inadmissible – §100a (4). This subsection states that these data shall not be used, shall be deleted without delay and the fact that they were obtained and deleted shall be documented, with a view to notification (§101 StPO). This provision is also provided for in section 20k of the BKAG (7), which states that, as far as possible, data related to the core area of private life should not be collected, and data that are collected must be screened and deleted by the Federal Data Protection Supervisor and two other

[254] See, e.g., Landgericht [District Court] Landshut, Beschluss vom 20. Januar 2011 – 4 Qs 346/10 -, juris.
[255] Art. 94, 98 & 100 StPO.
[256] Section 20k BKAG.
[257] Art. 100b subsection (1) StPO.
[258] Art. 100 StPO.

members of the Federal Criminal Police Office.[259] However, a 2016 judgement of the Federal Constitutional Court[260] determined these safeguards to be insufficient in the protection of the core area of private life. This judgement further stipulated that data should be screened by an independent body, albeit with leeway for "applicable exceptional cases in case of immediate danger".[261]

- Furthermore, the requests for authorisation must indicate certain data. In the StPO, data relevant to the identity and location of the person (where known), the telephone number or other code equipment (e.g. IMEI number / MAC number / IP address), and the type, extent and duration of the measure are needed – §100b (2). Section 20k of the BKAG stipulates the need for the person's name and address; the main reasons for the use of the measure; the most accurate description of the measure to be used; and the nature, scope and duration of the action, specifying the end date.[262]

Beyond these shared provisions, section 20k of the BKAG stipulates that the duration of the measure shall be limited to three months, with the possibility of an extension for no more than three months; that the measures must be terminated immediately if the conditions of the order are no longer fulfilled; and that the measure only undertakes actions that are indispensable to the order.

Provisions of the legal framework – *ex-post* considerations

In addition to the abovementioned *ex-ante* conditions, the StPO contains two key *ex-post* mechanisms of supervision and oversight of hacking practices:

i. **Notification of persons targeted:** As documented in StPO §101, it is a legal requirement to notify persons affected by a telecommunications interception order regardless of the use of the data collected in a criminal court case. It is stated in §101 (5) that "notification shall take place as soon as it can be effected"[263] without endangering the investigation, persons involved or significant assets. In cases of deferred notification, this must also be documented in the investigative file and approved by the court if deferral goes beyond 12 months. It is also necessary to delete and document the deletion of any personal data no longer necessary for the purposes of the criminal prosecution – pursuant to §101 (8). Furthermore, all means used in the investigation and all evidence collected – by law enforcement, the prosecution or the investigative judge – are required to be included in the investigation file. If the case goes to court, all elements of the file are made public to the court, where the legality and admissibility of the actions are determined and can be challenged – as stipulated in StPO §101 (7). If the case does not go to court, §101 still applies and persons must be notified. These provisions suggest strong oversight procedures. However, in some cases, persons who were not the intended target of investigative measures but were tangentially affected may not be notified – §101 (4).[264]

ii. **Reporting:** As detailed in StPO §100b (5) and (6), each Länder and the Federal Public Prosecutor General are required to submit an annual report to the Federal Office of Justice. These reports should include: i) the number of proceedings in which telecommunications interception measures were ordered; ii) the number of orders; and iii) the underlying criminal offence of the proceedings. The Federal Office of Justice is then

[259] Section 20k BKAG.
[260] BVerfG, Judgement of the First Senate of 20 April 2016 – 1 BvR 966/09 – paras. (1-360).
[261] BVerfG, Judgement of the First Senate of 20 April 2016 – 1 BvR 966/09 – paras. (1-360).
[262] Section 20k BKAG.
[263] Art. 101 (5) StPO.
[264] Art. 101 StPO.

required to produce a country-wide summary of these measures. These data are publicly available.[265]

Furthermore, pursuant to §100e, the Federal Government has a duty to annually report a selection of data points to the Federal Parliament. These data, amongst others, include the number of surveillance measures, the duration of each surveillance measure, whether persons concerned were informed and whether the surveillance produced results of relevance to the criminal proceedings.[266]

Beyond these provisions, the BKAG (§20k) stipulates additional safeguards, stating that any changes to the target information technology system must be automatically reversed as far as technically feasible; and that key information related to the technical means used shall be logged. The information to be logged includes: the designation of the technical means and its date of use; the organisational unit implementing the action; and information related to the identification of the target system and the collected data. Furthermore, §20k provides for the deletion of these logs at the end of a calendar year. This final point, however, was ruled to be unconstitutional by the abovementioned 2016 judgement due to the "very short period of time"[267] before deletion. The judgement states that "this period is so brief that […] neither a review by the Federal Data Protection Commissioner nor by the party concerned is likely to occur and the documentation of the deletion thus becomes meaningless".[268]

Fundamental rights considerations

Paragraph 95 of the European Court of Human Rights (ECtHR) judgement in Saravai v Germany stated the minimum safeguards that should be set out in a country's legislation to avoid abuses of power. Table 12 outlines how the German legal framework implements these safeguards.

Table 15: Legal implementation of ECtHR minimum safeguards in Germany

Minimum safeguards (ECtHR)	Legal implementation of safeguards in Germany
The nature of the offences which may give rise to an interception order.	Such measures are limited to serious crimes only in the StPO §100a (2) and danger to life/freedom/national security in BKAG §20k.
A definition of the categories of people liable to have their telephones tapped.	Such measures are targeted against suspects in a criminal investigation or those they are communicating with, as stated in StPO §100a (1) and (3) and BKAG §20k.
A limit on the duration of telephone tapping.	BKAG §20k stipulates a maximum limit of three months on the duration of a measure.
The procedure to be followed for examining, using and storing the data obtained.	BKAG §20k and the StPO stipulate procedure for the examination, use and storage of data. However, the German Constitutional Court ruled that the current safeguards for screening and deletion of information related to the core area of private life are insufficient.

[265] Art. 100b StPO – Official note: Statistics available at www.bundesjustizamt.de.
[266] Art. 100e StPO.
[267] BVerfG, Judgement of the First Senate of 20 April 2016 –1 BvR 966/09 – paras. (1-360).
[268] BVerfG, Judgement of the First Senate of 20 April 2016 –1 BvR 966/09 – paras. (1-360).

Minimum safeguards (ECtHR)	Legal implementation of safeguards in Germany
The circumstances in which recordings may or must be erased or the tapes destroyed.	BKAG §20k stipulates that certain logs related to the collection of data should be kept and deleted after a certain time period. However, the Constitutional Court ruled that the current time periods for retention and deletion do not serve to protect the target and deemed the provisions unconstitutional.

Technical means used for hacking by law enforcement

In relation to accessing protected data on a lawfully seized device, German law enforcement agencies are reportedly able to use whatever technical means are helpful – including both in-house and external capabilities.[269] For the use of hacking tools to intercept telecommunications data at source, however, there are slight restrictions as governed by case law on previous practices. In 2011, for example, an externally developed and acquired software was installed on a source laptop and used by law enforcement to intercept telecommunications data. However, this was criticised and determined to be illegal because the software had the ability to turn on the laptop's camera and microphone, even though the law enforcement agency did not use this functionality.[270] Since this incident, it is reported that the BKA no longer purchases external hacking expertise but develops and uses its own tools.[271]

Furthermore, the German Government does have expertise in hacking practices. The German Ministry of Interior has recently established a new authority – ZITiS – which will support German law enforcement and intelligence agencies through the provision of technical skills and expertise in these hacking practices. ZITiS will reportedly be staffed with 400 individuals.[272] Furthermore, the CCITÜ has existing capabilities in this area, as does the Federal Police and certain state criminal police forces. It is not clear how these entities will work alongside one another.

Hacking practices by the security services

Germany currently has three security and intelligence services. These are the Federal Office for the protection of the Constitution (*Bundesamt für Verfassungsschutz* – BfV), which deals with civil internal security; the Federal Intelligence Service (*Bundesnachrichtendienst* – BND), which has a mandate for both internal and external civil security; and the Military Counter-Intelligence Service (*Militärischer Abschirmdienst* – MAD), which covers military intelligence.

In 2016, two laws were passed related to the use of surveillance techniques, and thus hacking techniques, by German intelligence agencies. The Act to Improve Information Exchange in the Fight Against International Terrorism entered into force in July 2016 and the Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service was

[269] Franosch, R. 2017. Expert interview conducted for this study.

[270] Franosch, R. 2017. Expert interview conducted for this study; see http://www.spiegel.de/international/germany/spyware-scandal-merkel-s-cabinet-in-spat-over-trojan-horse-program-a-791455.html.

[271] Franosch, R. 2017. Expert interview conducted for this study; see http://www.sueddeutsche.de/politik/bundeskriminalamt-bundestrojaner-fuer-smartphones-und-tablets-1.3186711.

[272] Paganini, P. 2016. ZITiS is the new German Government cyber unit formed in the wake of terror attacks. Security Affairs article. http://securityaffairs.co/wordpress/50297/terrorism/zitis-german-cyber-unit.html.

adopted by the Bundestag in October 2016[273]. Furthermore, a budget report leaked to three media companies state that both the BfV and the BND are requesting significant 2017 budget increases of 18% and 12%, respectively.[274]

Civil society actors report that these laws extend the surveillance powers of the German intelligence services.[275] Furthermore, these actors criticise, in particular, the overly-broad permissible purposes of surveillance and the absence of judicial authorisation.[276]

[273] Library of Congress, Global Legal Monitor. 2016. Germany: Powers of Federal Intelligence Service Expanded.
[274] Knight, B. 2016. Germany to pour cash into mass surveillance. http://dw.com/p/1Jybl.
[275] EDRi. 2016. German surveillance laws: placebos, poison, and also bad sport. Article of 27 July 2016.
[276] Galvagna, C. 2016. German Foreign Intelligence Bill Fails Human Rights Standards.

Italy Country Report

Completed with the support of Professor Giovanni Ziccardi, Professor of Legal Informatics, University of Milan; and Professor Roberto Flor, Assistant Professor of Criminal Law and Professor of ICT Criminal Law and International Criminal Law, University of Verona.

Legal framework and context

It is widely acknowledged that Italian law enforcement agencies use hacking tools in the process of criminal investigations.[277,278] In fact, experts consider that the use of malware is the method of choice for Italy's law enforcement agencies. Simply put, malware is malicious software that is installed surreptitiously on the device of a third party, where it can then conduct a wide range of functions including monitoring and circumventing access controls, etc.[279] It is worth noting that, for such methods, "the doctrine usually refers only to Trojan horses or simply Trojans".[280]

Although the use of such tools has been established, the Italian legislative framework (namely, the Code of Criminal Procedure) has not been amended to take into consideration these technological advancements in investigative tools.[281] Consequently, improper legislation governing the use of these tools is likely to lead to breaches of the fundamental rights of Italian citizens.[282] Relevant rights are primarily provided for in the Italian Constitution and include:[283]

i. Privacy (Article 2, Italian Constitution and Article 8 of the European Convention on Human Rights);
ii. Inviolability of the digital domicile (Article 14, Italian Constitution); and
iii. Freedom and confidentiality of communications (Article 15, Italian Constitution).

To date, existing provisions in the Code of Criminal Procedure, intended for investigative procedures of an analogous nature, have been used as a legal basis for the use of trojans in criminal investigations. For example, a procedure for the interception of communications (via traditional investigative tools) in criminal investigations is well established in Italy; the use of trojans to intercept communications would use the same legal basis.

In addition, a range of case law decisions have guided the evolution of the use of hacking tools for criminal investigations.[284] These include:

[277] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

[278] Citizen Lab. 2014. Mapping Hacking Team's "Untraceable" Spyware. Accessed on 28.02.17 at: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

[279] Filiol, E. 2005. Computer Viruses: from theory to application. Springer.

[280] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

[281] Ziccardi, G. 2017. Expert interview conducted for this study.

[282] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

[283] Constitution of the Italian Republic. Official translation accessed on 28.02.17 at: https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf.

[284] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

- **Court of Cassation, 2009[285]:** this judgement legitimised the use of hacking tools to seize and copy documents stored on a device's hard disk without a search warrant from a judge;
- **Court of Cassation, 2012[286]:** this judgement further supported the 2009 decision, stipulating that an order by the Public Prosecutor was enough;
- **Court of Cassation, 2015[287]:** elements of the precedents set by the above judgements were, in effect, contradicted by this judgement, which ruled that specific conditions should be met if hacking tools are to be used for intercepting communications – e.g. the "surveillance should take place in clearly circumscribed places, identified at the outset, and not wherever the subject might be";[288]
- **Court of Cassation, 2016[289]:** as a result of these discrepancies, as similar case in 2016 referred the issue to the most authoritative session of the Court of Cassation (i.e. the 'Joint Sessions' – SS.UU.). The outcome of the 'Joint Sessions' was that the use of hacking tools is permitted for the interception of communications and, when it is not possible for the location to be identified individually and when criminal activities have not been committed, the use of hacking tools is only permitted for criminal proceedings on organised crime and terrorism. Furthermore, the decision separated the operational modes of hacking tools into two categories: 'online surveillance' and 'online search'. The former category relates to the interception of an information flow between devices (e.g. microphone, video, keyboard etc.) and the microprocessor of the target device. 'Online search' relates to copying the memory units of a computer system.[290]

These case decisions highlight some of the key issues and debating points related to the use of such tools in criminal investigations. Primarily, these decisions inform ongoing debates on the normalisation of the use of these tools. These discussions aim to strike a balance between the significant benefits brought by these tools, in terms of investigative efficiency, and the increased invasiveness of these tools. In addition, experts in the field argue that the normalisation of these activities should be prevented given that there are still significant challenges related to the collection of such evidence.[291] These challenges include[292]:

- Ensuring and demonstrating the chain of custody of evidence gathered via these means;
- Collecting evidence in another jurisdiction; and
- Limited expertise on the topic within the legal profession, thus hindering appropriate and consistent challenge of the use of these tools in court.

As a result of the use of trojans, the case law and the ongoing debates, several draft legislative proposals have been put forward in recent years. The first, a proposed amendment to a new law on terrorism from February 2015,[293] aimed to amend Article 266-bis of the Code of Criminal Procedure and was labelled 'misguided' by a prominent academic and criticised

[285] Italian Court of Cassation, Division V, Decision No. 24695, of 14 October 2009.

[286] Italian Court of Cassation, Division VI, Bisignani Case – Decision No. 254865, of 27 November 2012.

[287] Italian Court of Cassation, Division VI, Musumeci Case – Decision No. 27100, of 26 May 2015.

[288] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

[289] Italian Court of Cassation, Joint Sessions, Scurato Case – Decision No. 1 July 2016.

[290] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

[291] Ziccardi, G. 2017. Expert interview conducted for this study.

[292] *Id*.

[293] Decree-Law No. 7 of 18 February 2015, 'Misure urgenti per il contrasto al terrorismo anche di matrice internazionale'.

by several members of Parliament and the Prime Minister.[294] The second, the 'Greco' Bill of December 2015,[295] also tried to amend Article 266-bis and was also criticised.[296] The third, the 'Casson'[297] amendment, was developed in a different vein.[298] As noted by one expert, what emerges from these repeated attempts is the need to effectively regulate the use of trojans by law enforcement agencies.

A fourth, the so-called 'Quintarelli' draft law[299], was published in February 2017 after two years of development. As for the 'Casson' amendment, it approaches the issue differently in that: i) it proposes the insertion of relevant provisions into title III (*Mezzi di ricerca della prova*), book III of the Code of Criminal Procedure; and ii) it differentiates between the various functions of the trojan software, as the degree of invasiveness differs across the functions.[300]

Regarding point ii), experts in the topic have remarked that this element of the proposal was driven by technicians and not lawyers, as it adds significant specificity around the possible functions to be employed by law enforcement agencies.[301,302,303]

However, this legislative proposal is being driven by MPs from the Civici e Innovatori, a small parliamentary group with only 17 deputies in the Chamber of Deputies.[304] One academic expert remarked that this may impact the proposal's likelihood of acceptance.[305] The draft proposal is currently open to public consultation.[306] Given the novel and interesting elements included within this proposal, the following sections will detail the provisions currently proposed.

---

[294] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

[295] 'Greco' Bill, of 2 December 2015, Modifica all'articolo 266-bis del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche.

[296] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

[297] The bill and the related MP Casson amendment are available at http://parlamento17.openpolis.it/singolo_atto/53883.

[298] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

[299] Proposta di legge - "Atto camera 3762" QUINTARELLI ed altri: "Modifiche al codice di procedura penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, in materia di investigazioni e sequestri relativi a dati e comunicazioni contenuti in sistemi informatici o telematici" – work in progress

[300] Rules governing the use of government trojan with respect for individual rights: Summary of the proposed amendments to the Italian Code of Criminal Procedure. *Published 01.02.17.* Accessed on 28.02.17 at: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.

[301] Ziccardi, G. 2017. Expert interview conducted for this study.

[302] Pietrosanti, F. and Aterno, S. 2017. Italy unveils a legal proposal to regulate government hacking. Accessed on 28.02.17 at: http://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html.

[303] Moody, G. 2017. Italy Proposes Astonishingly Sensible Rules to Regulate Government Hacking Using Trojans. Accessed on 28.02.17 at: https://www.techdirt.com/articles/20170216/03431236726/italy-proposes-astonishingly-sensible-rules-to-regulate-government-hacking-using-trojans.shtml.

[304] Rules governing the use of government trojan with respect for individual rights: Summary of the proposed amendments to the Italian Code of Criminal Procedure. *Published 01.02.17.* Accessed on 28.02.17 at: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.

[305] Ziccardi, G. 2017. Expert interview conducted for this study.

[306] Rules governing the use of government trojan with respect for individual rights: Summary of the proposed amendments to the Italian Code of Criminal Procedure. *Published 01.02.17.* Accessed on 28.02.17 at: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.

Provisions of the legal framework – *ex-ante* considerations

This most recent draft law (February 2017) introduces a new investigative tool, termed "remote search and seizure" ("*Osservazione e acquisizione da remoto*"),[307] and aims to make the existing provisions for more traditional investigative tools (e.g. wiretapping) applicable to their modern-day equivalents.[308] To ensure that the use of this new tool and the pre-existing provisions are consistent with the abovementioned constitutional guarantees and human rights legislation, the draft law includes a range of *ex-ante* provisions.[309]

Authorisation for the use of this investigative tool must be obtained from the public prosecutor and subsequently validated by the judge presiding over a preliminary investigation. This authorisation should only occur if the judge considers the use of the tool to be "absolutely necessary"[310] for the continuation of the investigation, and that no other investigative means is sufficient.[311] It is also required that the authorisation details the specific functions that will be used, and thus protects against the overuse or abuse of a trojan's extensive functionalities.[312]

Further legislative provisions include:[313]

- Use of the tool is "strictly limited" to investigations into organised crime, and targeted to individuals or a specific setting (e.g. room, building)[314];
- Data accessed using such a tool "must be stored in the prosecutor's servers and must be protected from third-party access" with encryption[315]; and
- Non-relevant data must be screened and deleted.

Some of the most innovative provisions, described by one critic of the use of hacking tools by law enforcement as "astonishingly sensible",[316] relate to the trojan tools. Primarily, as alluded to above, the proposed law aims to map the functionalities of the trojans to the relevant existing articles of the Code of Criminal Procedure. For example, "digital tailing" is included within the same article as "physical tailing".

Moreover, in terms of *ex-ante* provisions, the draft law stipulates that:

- Trojans must be directly operated by law enforcement (i.e. not private contractors);
- Every operation that uses a trojan must be duly logged and documented in a tamperproof, verifiable way such that the operation's results can be fairly contested by the defendant; and
- Once installed, a trojan shall not reduce a device's security level.

---

[307] *Id.*

[308] Pietrosanti, F. and Aterno, S. 2017. Italy unveils a legal proposal to regulate government hacking. Accessed on 28.02.17 at: http://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html.

[309] Ziccardi, G. 2017. Expert interview conducted for this study.

[310] Rules governing the use of government trojan with respect for individual rights: Summary of the proposed amendments to the Italian Code of Criminal Procedure. *Published 01.02.17.* Accessed on 28.02.17 at: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.

[311] *Id.*

[312] Pietrosanti, F. and Aterno, S. 2017. Italy unveils a legal proposal to regulate government hacking. Accessed on 28.02.17 at: http://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html.

[313] Rules governing the use of government trojan with respect for individual rights: Summary of the proposed amendments to the Italian Code of Criminal Procedure. *Published 01.02.17.* Accessed on 28.02.17 at: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.

[314] Ziccardi, G. 2017. Expert interview conducted for this study.

[315] Pietrosanti, F. and Aterno, S. 2017. Italy unveils a legal proposal to regulate government hacking. Accessed on 28.02.17 at: http://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html.

[316] Moody, G. 2017. Italy Proposes Astonishingly Sensible Rules to Regulate Government Hacking Using Trojans. Accessed on 28.02.17 at: https://www.techdirt.com/articles/20170216/03431236726/italy-proposes-astonishingly-sensible-rules-to-regulate-government-hacking-using-trojans.shtml.

Provisions of the legal framework – *ex-post* considerations

In addition to the above *ex-ante* provisions, the draft law proposes a range of *ex-post* supervisory provisions.

Within the course of an investigation, any use of these tools is secret from the target. However, there is a requirement to notify individuals that have been the subject of invasion by such tools.[317] Furthermore, evidence will not be admissible if collected in a way that is deemed to be outside the scope of the judge's authorisation and the punishment for abusive use of these tools has increased.[318]

Furthermore, case-relevant and general provisions aiming to safeguard the use of the tools, along the same lines as those mentioned above, have been included in the draft law. These include:[319]

- Once an investigation has finished, the trojan must be safely removed from the target device(s) – either by law enforcement or through detailed instructions;
- Trojan production and use must be traceable. It is proposed that this is done through a National Trojan Registry, which would hold a 'fingerprint' of each version of the software;
- A trojan's source code must be deposited to a specific authority and must be verifiable with a reproducible build process (in a similar fashion to Debian Linux); and
- Trojans must hold an annually reviewed certificate to ensure compliance with law and technical regulation.

Fundamental rights considerations

The abovementioned conditions provide for many of the relevant and expected fundamental rights safeguards. These conditions include: limiting the use of hacking tools to criminal investigations related to organised crime; protecting against the overuse of hacking tools by separating the functionalities of trojans; the requirement to notify targets; the secure storage of data and the deletion of non-relevant data; and the comprehensive system proposed for monitoring the use and development of hacking tools for law enforcement.

However, an academic expert reported that the use of these tools, and the evidence gathered, is not challenged in court as many legal professions do not have enough knowledge of the tools and how evidence is gathered using these tools.[320] Furthermore, the requirement to delete 'non-relevant' data does not define this term and it does not provide for the fact that the investigator may already be cognisant of this data,[321] i.e. the 'fruit of the poisoned tree' doctrine.

Technical means used for hacking by law enforcement

As mentioned above, it is widely known that the Italian judiciary has been ordering remote interceptions and remote digital extractions for some years. The technique of choice is the surreptitious installation of hidden malware known as trojan horses.[322] Currently, the legislation does consider the technological advancements that allow the extraction,

[317] Rules governing the use of government trojan with respect for individual rights: Summary of the proposed amendments to the Italian Code of Criminal Procedure. *Published 01.02.17.* Accessed on 28.02.17 at: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.

[318] Ziccardi, G. 2017. Expert interview conducted for this study.

[319] Pietrosanti, F. and Aterno, S. 2017. Italy unveils a legal proposal to regulate government hacking. Accessed on 28.02.17 at: http://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html.

[320] Ziccardi, G. 2017. Expert interview conducted for this study.

[321] Ziccardi, G. 2017. Expert interview conducted for this study.

[322] Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

interception, etc., of data by digital means. However, the draft legislation proposed in February 2017 stipulates some novel provisions regarding the tools to be used by law enforcement agencies.[323]

First, these provisions aim to legally separate the functionalities of a trojan such that they require separate authorisation. Among the functions stipulated are 'digital tailing', voice interception and video / sound recording. Second, the provisions provide for extensive monitoring of the use and development of trojans. Third, these trojans must be directly operated by law enforcement, and not by private contractors.[324]

It is also known, however, that Italian companies are proficient developers of such tools, the most notable being Hacking Team, and have previously provided such tools to the Italian government. Therefore this legislative proposal, if accepted, will place a range of obligations on private companies if they continue to provide these services (e.g. depositing the source code). An academic expert noted that the economic and intellectual property value of a company's source code may prevent them from collaborating in this way in the future.[325]

Hacking practices by the security services

Italy currently has three security and intelligence services. These are the Information and Internal Security Agency (*Agenzia informazioni e sicurezza interna* – AISI), which holds a mandate for internal civil security; the Information and External Security Agency (*Agenzia informazioni e sicurezza esterna* – AISE), which covers external civil security; and the Department of Information and Security (*Reparto informazioni e sicurezza* – RIS), which accounts for military intelligence.[326]

In 2007, the Italian Parliament launched an extensive reform of the intelligence agencies in Italy through Law nº 124 of 3 August 2007 on Information System for the security of the Republic and new rules on State secrets. Oversight of activities conducted under this law by the abovementioned security and intelligence services is primarily conducted by the Parliamentary Committee for the Security of the Republic (COPASIR). This Committee is tasked with systematically and continuously verifying that the activities of the agencies are in accordance with "the Constitution, the laws, solely in the interest and for the defence of the Republic and its institutions"[327]. As such, extensive provisions for oversight, supervision and reporting are stipulated.

However, there are a range of criticisms of this system. For example, the law does not provide for notification or specific judicial or non-judicial remedies for subjects of surveillance.[328] Furthermore, the law does not expressly state the nature of circumstances which may result in the use of hacking techniques; does not express the need for an ex-ante or ex-post warrant; and does not limit the duration or geographical scope of hacking practices.[329]

---

[323] Rules governing the use of government trojan with respect for individual rights: Summary of the proposed amendments to the Italian Code of Criminal Procedure. *Published 01.02.17.* Accessed on 28.02.17 at: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.

[324] *Id.*

[325] Ziccardi, G. 2017. Expert interview conducted for this study.

[326] European Union Agency for Fundamental Rights. 2015. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member States' legal frameworks.

[327] Gambini, M. 2014. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: ITALY.

[328] *Id.*

[329] *Id.*

Netherlands Country Report

Completed with the support of Dr. Jan-Jaap Oerlemans, guest lecturer at the Center for Law and Digital Technologies, University of Leiden; and Ton Siedsma, Bits of Freedom.

Legal framework and context

The **current legal basis for lawful hacking (remote access) has been debated over the past few years**. Dutch law requires that investigative methods that interfere with the involved individuals' rights and freedoms in more than a minor manner or threaten the integrity of the criminal investigation are based in specific provisions in Dutch criminal procedural law.[330] In a letter announcing plans for a new law on combating cybercrime of 2012,[331] the Ministry of Security and Justice explained that although Article **125i of the Dutch Code of Criminal Procedure** allowed law enforcement to search a place with the aim to secure data stored on a computer, parliamentary history implied that entering or searching an "computerised device" remotely was not permitted. As a result, the Ministry was proposing a new piece of legislation which would provide for this legal basis.

However, in May 2014 the Dutch Public Prosecution Office announced that, as part of a large-scale investigation into the Blackshades malware coordinated by Eurojust, the Dutch police Team High Tech Crime remotely accessed and entered the server of Blackshades to copy data, without knowing the location of the server.[332] Prompted by parliamentary questions, the Minister of Security and Justice confirmed the hacking by the Dutch police, stating as the legal basis Article 125i Dutch Code of Criminal Procedure. The Minister further stated that under certain circumstances accessing computerised devices remotely, with the aim to search it and copy data, was already allowed under Article 125i, with the authorisation from the investigative judge.[333]

However, some experts in the field do not agree with this statement. Expert Jan-Jaap Oerlemans from the University of Leiden argues that Dutch criminal procedural law currently does not include any special investigative power that distinctly regulates the investigative power for remotely accessing computer systems after which a remote search can be conducted or policeware can be installed on the accessed computer. He further stated that Article 125i refers to existing investigation powers for search and seizure at a particular place by law enforcement authorities (i.e. a physical search, not remotely)[334] and that Dutch legislature did not intend to provide Dutch law enforcement authorities with the power to hack computers.[335] Moreover the fact that the Minister stated that prior authorisation is needed by the investigative judge for undertaking hacking by law enforcement, which is not required under Article 125i, suggests an acknowledgement on the part of the government that remote access is a heavier investigative tool.[336] Oerlemans is therefore of the opinion

---

[330] Oerlemans, J.J. Investigating cybercrime, Chapter 8: Performing hacking as an investigative method, January 2017, p. 250.

[331] Ministerie van Veiligheid en Justitie, Briefa an de Voorzitter van de Tweede Kamer « Wetgeving bestrijding cybercrime », 15 October 2012. Available here: https://www.rijksoverheid.nl/documenten/kamerstukken/2012/10/15/wetgeving-bestrijding-cybercrime.

[332] See: https://www.om.nl/vaste-onderdelen/zoeken/@85963/wereldwijde-actie/

[333] Vragen van de leden Berndsen-Jansen en Verhoeven (beiden D66) aan de Minister van Veiligheid en Justitie over het hacken van servers door de politie terwijl de zogenaamde «hackwet» nog niet door de Kamer is behandeld (ingezonden 26 augustus 2014). Antwoord van Minister Opstelten (Veiligheid en Justitie) (ontvangen 20 oktober 2014). Zie ook Aanhangsel Handelingen, vergaderjaar 2013–2014, nr. 34. Available here: https://zoek.officielebekendmakingen.nl/ah-tk-20142015-286.html.

[334] Oerlemans, J.J. Investigating cybercrime, Chapter 8: Performing hacking as an investigative method, January 2017, pp. 226-261.

[335] Oerlemans, J.J. Hacken als opsporingsbevoegdheid, 2011, pp. 901-903. See also B.J. Koops & Y. Buruma (2007), 'Formeel strafrecht en ICT', in: B.J. Koops (red.), *Strafrecht en ICT*, 2e druk, Den Haag: Sdu 2007, p. 118.

[336] Oerlemans, J-J. 2017. Expert interview conducted for this study.

that the statement of the Minister of Security and Justice is worrisome, because a special investigation power was interpreted very broadly by the Minister to suit the needs of law enforcement authorities, undermining the criminal procedural legality principle of the Dutch criminal law system.[337] Bits of Freedom,[338] a Dutch digital rights NGO, also argued that 125i does not provide for a legal basis for remote access of servers and copying data for investigative purposes.

Finally, jurisprudence does not provide for any clarification on the legal basis either, as no case on lawful hacking has ever been decided on in court.[339]

It should be noted that a special investigative power is available for **network searches**, which is the entering of computers on the same network, when investigating a computer in the context of a (physical) search.[340] Moreover, Dutch law **prohibits the buying of zero-day vulnerabilities**, but according to the Ministry of Security and Justice it is allowed to buy hack tools that use zero-day vulnerabilities.[341]

The **Computer Crime III Act, informally also called the Hacking Law, is a legislative proposal currently being considered which aims to regulate hacking as an investigation power.**[342] This explicitly regulates remote searches, the use of policeware, and other forms of hacking, as an investigative method (but not network searches), as a special investigative power. The law is accompanied by a 124-page Explanatory Memorandum, which further explains and provides an interpretation of the proposed amendments.

As stated above, the proposed law was announced in the letter of the Ministry of Security and Justice in 2012. In June 2013, a public consultation took place, which resulted in 37 responses. In December 2015, the proposal was sent to Parliament for a public hearing.[343] On 13 December 2016, the Parliament debated the proposed hacking law. A week later, on 20 December, the Parliament voted in favour of adopting the proposed law. The Computer Crime III Bill will now be debated in the Senate and is likely to be adopted between the summer of 2017 and early 2018.

The proposal would grant Dutch law enforcement agencies the power to:

- Remotely access/hack electronic devices, which may or may not be connected to the internet.
- After accessing the device: search the device, to activate applications (including webcams and microphones), to copy or delete data.

The above is laid down in the new **Art 126nba** of the Code of Criminal Procedure, as proposed in the Computer Crime III Bill.

The proposed law has also been heavily debated. The debate mostly revolved around vulnerabilities. Although Dutch law does not allow zero-day vulnerabilities to be bought commercially by law enforcement, it does allow the police to buy software which uses such vulnerabilities, as long as the vulnerabilities are reported to the creator of the vulnerable

[337] Oerlemans, J-J. 2016. Hacking without a legal basis, Leiden Law Blog, 30 October 2016. Available at: http://leidenlawblog.nl/articles/hacking-without-a-legal-basis.

[338] See: https://www.bof.nl/category/hackvoorstel/.

[339] Oerlemans, J-J. 2017. Expert interview conducted for this study.

[340] Oerlemans, J-J. 2017. Investigating cybercrime, Chapter 8: Performing hacking as an investigative method. Available here: https://openaccess.leidenuniv.nl/bitstream/handle/1887/44879/08.pdf?sequence=11.

[341] https://tweakers.net/nieuws/118953/staatssecretaris-politie-mag-hacktools-kopen-die-gebruikmaken-van-zero-days.html.

[342] Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III).

[343] Wetsvoorstel Computercriminaliteit bij Tweede Kamer ingediend, 22 December 2015.

software. Bits of Freedom argues in this regard that in cases where these unknown vulnerabilities are exploited via governmental malware, the police are either not aware of the vulnerability (and thus cannot notify) or are bound to a non-disclosure agreement (and thus are not allowed to notify). Consequently, law enforcement agencies will either break the law or break their contract.[344] According to Bits of Freedom, the use of not publicly known vulnerabilities to access devices of suspects would leave innocent users of the same type of devices vulnerable to the illicit exploitation of those same vulnerabilities, and might ultimately lead to more cybercrime.

Moreover, Bits of Freedom is of the opinion that although it is a positive development that a law is being adopted on this topic for the purpose of legality, the proposed law is too broad and too far reaching:[345]

- The term 'computerised device' is defined too broadly and could include a range of different smart devices connected to the internet (further explained below). The terminology was based on Article 1 of the Cyber Crime Convention.
- Even though the Explanatory Memorandum to the new law states these investigative powers should only be used in exceptional cases, this is not stated in the law itself: the investigative powers (incl. turning on webcams remotely) can be used for any criminal offence which carries a sanction of four years or more (so not only terrorism and cybercrime), if it is considered to "seriously breach the rule of law".
- There is a risk that the investigative judge that needs to provide for the required authorisation does not have enough knowledge of each case for which legal hacking is requested, which carries a risk of abuse of the investigative power.

Provisions of the legal framework – *ex-ante* considerations

The proposed Computer Crime III Act does include the requirement for the public prosecutor to submit a written request asking for a written prior authorisation (*machtiging*) to the investigative judge, before giving an order for hacking.[346] The authorisation needs to state the details of the hacking order and the period for which hacking is authorised. However, while the start of a hacking operation requires prior written authorisation, the proposed Article 126nba (5) allows that extensions of the authorisation of the investigative judge can be provided orally in "urgent need", as long as the authorisation for the extension is eventually provided in written form within three days.

The decision is taken on the basis of a proportionality assessment and both the request by the public prosecutor and the authorisation decision of the investigative judge must be motivated on this basis. The Explanatory Memorandum of the proposed new law further requires the Central Review Commission (*Centrale Toetsings Commissie*) to provide advice to the investigative judge before it takes its decision. Moreover, the technical means proposed are assessed against several legal safeguards under the 2006 Decree of technical tools.[347]

Article 126nba (3) of the proposed Computer Crime III Act states that the order for the special investigative power of hacking can only be provided for a maximum period of four weeks, and can be extended for a maximum period of four weeks at a time.

---

[344] Siedsma, T. Bits of Freedom. 2017. Expert interview conducted for this study.

[345] Siedsma, T. Bits of Freedom. 2017. Expert interview conducted for this study.

[346] Artikel 126nba (4), Gewijzigd Voorstel van Wet – Computercriminaliteit III, 20 December 2016.

[347] Besluit technische hulpmiddelen strafvordering, available here: http://wetten.overheid.nl/BWBR0020444/2013-03-15.

Article 126nba (2) of the proposed Computer Crime III Act requires the prosecutor's order for law enforcement to hack as part of an investigation to include the following details:

- The alleged crime and (if known) the name of the suspect;
- The number or another identifying description of the computerised device to be hacked;
- The circumstances which show that the crime is a 'serious breach of law' and that the investigation needs the hacking 'urgently'.
- A description of the type and functionality of the technical means to be used;
- The purpose of the hacking and, in some cases,[348] a description of the acts to be undertaken;
- Which part of the computerised device and which categories of data are included;
- The time or time period for which the order is given;
- Whether or not a technical means is to be applied on a person.

Under the proposed Article 126nba of the Code of Criminal procedure,[349] hacking can only be requested by the public prosecutor for investigations:

- into crimes described in **Article 67(1)** of the Dutch Code of Criminal Procedure (crimes for which the maximum sentence is four years or higher, or some specifically designated crimes with a lower maximum); and
- into crimes that are **serious breaches of law;** and
- when **the investigation requires this urgently**; and
- for the purpose of:
    - establishing certain characteristics of the automated device of the user (e.g. the identify or location);
    - to execute an order as described in Article 126l (recording private communications by using a technical aid) or 126m of the Criminal Procedure Code (recording private communications which take place using services provided through a communications provider, by using a technical aid);
    - to execute an order as described in Article 126g of the Criminal Procedure Code (systematic observation, incl. by attaching a technical aid to a person);
    - recording of data that are stored in the automated device;
    - making data inaccessible (as described in Article 126 cc (5) of the Criminal Procedure Code)

In practice this article (also looking at the Explanatory Memorandum) would allow law enforcement to **enter** a computerised device that is used by the suspect and **search** the device with the purpose of:

- Undertaking an online search (stored data), including looking at the data and copying the data, as well as making data inaccessible.
- Intercepting private information (streaming data), including capturing key strokes (incl. passwords) and real-time monitoring of data traffic (which may or may not include encryption).
- Influencing the data, by adjusting settings, turning on webcams / microphones, sabotaging or turning a device off.

Moreover, the law would allow law enforcement to provide itself with access to / enter the computerised device in different ways, including:

- Using a vulnerability in the IT system;
- Enter / intrude using a false identity or by brute force.

[348] If for the purpose of article 126nba (1) 9a), (d) or (e) Wetboek van Strafvordering.

[349] Artikel 126nba, Gewijzigd Voorstel van Wet – Computercriminaliteit III, 20 December 2016.

- Use a trojan to infect the device with malware.[350]

If the hacking is undertaken for the purpose of copying or deleting stored or incoming data, the offence to which the hacking relates needs to be an offence which carries a sentence of eight years or more.

What can be searched (e.g. information relating to the core area of private life) will depend on the particular circumstances of the case. Moreover, case law and the Explanatory Memorandum of the new proposed law require that the hacking needs to be proportional to the breach of the right to private life of the suspect or third parties by using the investigative power (**proportionality test**). Moreover, it requires that the evidence that will be gathered through the hacking cannot be gathered by using another less intrusive investigative power (**subsidiarity test**). Hacking should be **targeted to an individual**: the request made will concern a particular individual for one particular investigation (although it could concern multiple computers that belong to the same individual; it may also involve computers belonging to others provided that the suspect uses these with some frequency).

The Explanatory Memorandum of the new proposal states that law enforcement agencies are also allowed to hack a foreign server, as long as the location of the server is unknown.[351] However, if the Dutch police are aware of where the server is located, then the law enforcement authorities are required to send a request for legal assistance to the country where the server is based. If the country does not respond to such request, the Dutch police may hack the server.

The information collected through hacking may be used as evidence during the criminal investigation and during the trial. The Memorandum of Understanding of the proposed hacking law states that in order to check which hacking activities were undertaken, law enforcement needs to log their hacking activities in the automated device.[352] It further states that the requirements around this 'logging' will be included in the Decision on technical aid (Besluit technische hulpmiddelen strafvordering) (the Memorandum also notes that any activities undertaken by the police officer need to be included in the 'proces-verbaal' (a statement of the facts of the case), referring to Article 152 of the Dutch Code of Criminal Procedure. However, the statement does not include information on the software that was used to undertake the hacking.

Provisions of the legal framework – *ex-post* considerations

The national law does not require *ex-post* supervision or oversight by judicial or other bodies, but assumes that *ex-post* oversight will take place when the case goes to trial and the evidence resulting from the investigation measures is tested in court. The new Computer Crime III Bill does have a provision (art. 126nba (7)) foreseeing *ex-post* monitoring by the Inspection of Public Order and Safety (*Inspectie Openbare Orde en Veiligheid).*[353] However, according to Bits of Freedom this oversight is not independent judicial oversight as described in European jurisprudence. Moreover, the law is unclear on what the oversight by this Inspection would exactly entail.[354]

As stated above, the 'proces-verbaal', which is a statement of the facts of the case, includes information on the special investigative powers, such as hacking, used in the particular case. The suspect and his/her lawyer can take note of this document in preparation for the trial.

---

[350] Siedsma, T. Bits of Freedom. 2017. Expert interview conducted for this study.
[351] Memorie van Toelichting Wet Computercriminaliteit III, 2015, pp. 47-48.
[352] Memorie van Toelichting Wet Computercriminaliteit III, 2015, Section 2.6.
[353] See also article 65 Politiewet.
[354] Siedsma, T. Bits of Freedom. 2017. Expert interview conducted for this study.

In the event that they perceive these investigative powers to be used unlawfully, they could argue this in court.

There is no parliamentary oversight for lawful hacking by the police in the Netherlands (this only exists for hacking by the secret services).[355]

The new Dutch law places an obligation on law enforcement agencies to notify the suspect of their use of hacking once the investigation is over and insufficient evidence has been found to continue the investigation or to bring the case to court.[356] Another way for the use of the hacking power by the police to become public is if the case goes to court and one of the grounds of the lawyer was the unlawful use of the investigative power of hacking (procedural defect) and the judgement is made public.

The provisions of the new proposed Computer Crime III Act are specific in terms of the purposes the hacking can serve (to capture information, to copy information, etc.). However, according to Bits of Freedom the term 'computerised device' is too broad, and technically could include smart cars or smart fridges or even pacemakers (also mentioned in the Explanatory Memorandum).[357] In the commentary to the proposed hacking law, the government states that it does not foresee the police hacking into pacemakers, and that this would not be allowed as it would not be proportional.[358]

Fundamental rights considerations

Fundamental rights safeguards that are in place within the new proposed Computer Crime III Act are (of which some were already in place under the existing law):

- The obligation for law enforcement to notify the person against which such legal hacking has been used[359]: However, according to the NGO Bits of Freedom this obligation is not being complied with systematically in practice. An evaluation from the Dutch Research and Documentation Centre (WODC) from 2004 confirmed that the duty of notification laid down in Article 126bb of the Criminal Procedure Code was complied with on a limited scale, that a clear policy was lacking amongst prosecutors and that notification only happened incidentally.[360] However the WODC concluded in 2011 that the researched prosecutor services did generally comply with the duty of notification in 2011, even though it was implemented differently.[361] Several respondents from one investigated region reported that notification had had a low priority for years, but that no pressure was exerted by the Ministry of Justice to comply with this duty;
- The fact that law enforcement agencies are prohibited from buying zero-day vulnerabilities and have an obligation to report exploited vulnerabilities to the relevant organisation[362]: However according to Bits of Freedom, law enforcement can buy software which exploits known and unknown vulnerabilities and may have signed an NDA with the companies selling the malware exploiting these vulnerabilities, effectively blocking the obligation to notify in practice)[363];

---

[355] Oerlemans, J-J. 2017. Expert interview conducted for this study.

[356] Article 126bb Wetboek van Strafvordering.

[357] Oerlemans, J-J. and Siedsma, T. 2017. Expert interviews conducted for this study.

[358] Memorie van Toelichting Wet Computercriminaliteit III, 2015.

[359] Article 126bb Wetboek van Strafvordering.

[360] WODC, De Wet bijzondere opsporingsbevoegdheden – eindevaluatie, 2004. P.145. Available here: https://www.wodc.nl/binaries/ob222-volledige-tekst_tcm28-74925.pdf.

[361] WODC, Het gebruik van de telefoon- en internettap in de opsporing, 2012, p.16. Available here: https://www.rijksoverheid.nl/documenten/kamerstukken/2012/05/25/wodc-rapport-het-gebruik-van-de-telefoon-en-internettap-in-de-opsporing.

[362] Article 126ffa Wetboek van Strafvordering.

[363] Siedsma, T. Bits of Freedom. 2017. Expert interview conducted for this study.

Moreover, the Explanatory Memorandum to the proposed Computer Crime III Act states that individuals that have been hacked by law enforcement can make a claim for damages if the hacking caused harm (e.g. the computerised device that was hacked breaks down, causing data loss) for which law enforcement is liable[364]: however, again in practice, if the hacked individuals are not notified in practice (as discussed above) and therefore unaware that they were hacked by the police, this article becomes a dead letter.

Bits of Freedom further noted that the lack of notification of the persons that have been hacked, in combination with the hacking of foreign servers, has resulted in very few cases on the use of these investigative hacking methods coming before the Dutch courts.[365]

More generally, the Netherlands is a signatory of the European Convention on Human Rights and therefore needs to abide by Article 6 (right to a fair trial) and Article 8 (respect to private life).

Technical means of law enforcement authorities undertaking lawful hacking

In terms of the techniques, tools and methods used by law enforcement agencies when undertaking hacking practices, no information has been provided by the government. In 2013, the Director of Bits of Freedom submitted a freedom of information request asking about the use of these types of software by the Dutch law enforcement, but was told that no documents existed on this topic.

In August 2014, the media reported that the Dutch government was found on a list of clients of Gamma International, the company that sells the hacking software FinFisher, suggesting that the police would use three types of Gamma's software, with a licence running from 2012 to 2015.[366] As a result, questions were asked by a member of Parliament to the Ministry of Security and Justice on the use of spy software by law enforcement.[367] The Dutch government answered in this regard that providing details about what specific software is used by the investigative services of the police would bring great risks in terms of the use of those tools and that the police, in the acquisition of such tools, are bound by secrecy and that therefore no further information could be provided.[368]

As stated above, the Dutch law prohibits the purchase of vulnerabilities, but allows the procurement of off-the-shelf tools that exploit known and unknown vulnerabilities. As stated above, the Dutch law includes an obligation to report exploited vulnerabilities to the organisation with the vulnerability.

Hacking practices by the security services

In 2002, the Dutch legislature explicitly created hacking powers for Dutch national security and intelligence services (*Algemene Inlichtingen- en Veiligheidsdienst* or AIVD) in Article 24 of the Intelligence and Security Services Act of 2002. In February 2017, the Parliament voted in favour of a proposed piece of legislation that would replace the 2002 Act.[369] The new law would allow the intelligence services to hack through third parties (i.e. hacking person A to get to person B). However, the law does not specify the tools, techniques and methods the security services will be allowed to use.[370]

---

[364] Memorie van Toelichting Wet Computercriminaliteit III, 2015, p. 37.

[365] Siedsma, T. Bits of Freedom. 2017. Expert interview conducted for this study.

[366] http://www.volkskrant.nl/vk/nl/2664/Nieuws/article/detail/3715207/2014/08/08/Politie-gebruikt-mogelijk-omstreden-spionagesoftware.dhtml.

[367] https://zoek.officielebekendmakingen.nl/ah-tk-20142015-202.html.

[368] https://zoek.officielebekendmakingen.nl/ah-tk-20142015-202.html.

[369] https://www.aivd.nl/onderwerpen/nieuwe-wet-op-de-inlichtingen--en-veiligheidsdiensten.

[370] Siedsma, T. Bits of Freedom. 2017. Expert interview conducted for this study.

Poland Country Report

Completed with the support of Marta Przywała, Magdalena Szwiec (the Kosciuszko Institute) and Prosecutor Paweł Opitek.

Legal framework and context

The phenomenon of hacking is presented and penalised as a crime through the **Polish Penal Code**.[371] Article 267 of the Penal Code provides for several offences, defining them as:[372]

i. *Whoever without authorization obtains access to an information not meant for them, by opening a sealed letter, connecting into a telecommunications network, or by breaking or avoiding electronic, magnetic, informatic or other special protection of such network shall be punished by imprisonment of up to two years.*
ii. *The same penalty shall apply to anyone who without authorization obtains access to the whole or a part of an informational system.*
iii. *The same penalty shall apply to whoever with an aim of obtaining information to which they are not authorized uses eavesdropping, visual or other tools or programs.*
iv. *The same penalty shall apply to whoever reveals information obtained by means described in 1-3 to another person.*
v. *Offences described in 1-4 are prosecuted upon the request of the victim.*

However, 'unauthorised access' is an ambiguous term, not legally defined and allowing for a great deal of flexibility.[373] Obtaining access to an information system is not dependent on any specific method. It simply means taking over control of the information system.[374] This control gives the perpetrator the possibility to view, copy, block, delete or otherwise use the information stored in the information system, but it is not relevant whether they undertake any of these actions as the mere possibility constitutes access.[375] Access to the whole information system is not necessary; access to a part of it suffices to constitute the offence.[376] Similarly, obtaining information, the key element of *actus reus* in paragraphs i and iii above, is defined as obtaining the freedom to dispose with the information, whether by controlling the physical device in which it is stored or by copying it or simply by learning its content.[377]

Consequently, the terminology used regarding law enforcement practices does not refer to hacking. This is the case in both Polish legislation and legislative literature. However, as illustrated in Judgement K23/11 of the Polish Constitutional Tribunal, 'operational surveillance'[378] activities (referring to various means of law enforcement accessing communications data, including means that would be considered 'hacking') were already one of the "commonly accepted instruments for detecting threats and prosecuting the breaches of law".[379] Subsequently, this judgement determined that the existing legal provisions – contained within the **Polish Act on Police of 6 April 1990**[380] – were insufficient and

[371] Polish Penal Code: Act of 6 June 1997.

[372] Polish Penal Code: Act of 6 June 1997, art. 267. *Unofficial translation provided by study expert, Ivan Skorvánek.*

[373] Adamski, Andrzej. 2015. 'Cybercrime Legislation in Poland', *National Report for the International Congress on Comparative Law*, p. 10.

[374] Adamski, Andrzej. 2008. Opinion on the draft law no. 458 amending the Criminal Code, Biuro Analiz Sejmowych, p. 6.

[375] Sakowicz, Andrzej, 'Art. 267' in Michał Królikowski, Robert Zawłocki (eds.), *Kodeks karny. Część szczególna. Tom I. Komentarz do artykułów 117–221*, C.H. Beck (2013), p. 439.

[376] *Id.*, p. 442.

[377] *Id.*, p. 439.

[378] Judgment K 23/11 of the Constitutional Tribunal of 30 July 2014. 80/7/A/2014. Official translation accessed on 10.02.17 at: http://trybunal.gov.pl/en/hearings/judgments/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/.

[379] *Id.*

[380] Polish Act on the Police of 6 April 1990.

recommended a range of key amendments, to be implemented within 18 months of the decision (i.e. by 7 February 2016).[381]

November 2015 saw a new Parliament in Poland and, as no amendments had been passed, there was limited time to transpose the recommendations of the judgement. As such, the new amendments were developed and voted into being by means of an accelerated procedure. Of key relevance to this country report is the new Article 19 of the Act on Police, which governs 'classic' surveillance activities.[382]

Therefore, Polish legislation provides for law enforcement practices that have the purpose of circumventing the security of ICTs. However, the new legislative provisions have received extensive criticism – most notably by the Council of Europe's Venice Commission[383] – as they reportedly do not fully implement all the recommendations of the Polish Constitutional Tribunal regarding protection of the right to privacy.

Additional legislation of relevance includes the **Polish Code of Criminal Procedure of 6 June 1997**[384] – which includes a separate legal regime on surveillance for criminal investigations – and the **Act of 10 June 2016 on anti-terrorist activities**,[385] which stipulates the powers of the Internal Security Agency (ISA), Poland's domestic intelligence agency.

Provisions of the legal framework – *ex-ante* considerations

As mentioned above, the technical means by which law enforcement agencies can lawfully circumvent the security of ICTs within **preliminary investigations** are governed primarily by **Article 19 of the Act on Police**.[386] Article 19 §6 stipulates what 'operational controls' – the terminology used by the Act – are permitted. It specifies that "operational controls are performed confidentially"[387] before stating that they consist of:

i. *Extracting and recording the content of conversations carried out using technical resources, including telecommunications networks;*
ii. *Extracting and recording images and sounds of people in inside spaces, transport or any non-public places;*
iii. *Extracting the content of correspondence, including correspondence exchanged through electronic means of communication;*
iv. *Extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems; and*
v. *Gaining access to and checking the contents of mail.*[388]

Furthermore, **Article 14 §4** governing the scope of Police powers stipulates that "*in order to fulfil their statutory duties the Police may utilise personal data, **including electronic data**,*

[381] *Id.;* see Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016 for a summary, pp. 5-6.

[382] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016.

[383] *Id.,* p. 31.

[384] Polish Code of Criminal Procedure, Act of 6 June 1997. Unofficial translation accessed on 10.02.17 at: http://www.legislationline.org/documents/section/criminal-codes/country/10.

[385] Polish Act of 10 June 2016 on anti-terrorist activities and on the amendments to other acts. Unofficial translation accessed on 09.02.17 at: http://www.legislationline.org/topics/country/10/topic/5.

[386] Polish Act on the Police of 6 April 1990.

[387] *Id.*, Article 19 §6.

[388] Poland: Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Translation by the Council of Europe, accessed on 10.02.17 at: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)036-e.

obtained by other authorities, services and state institutions in the course of preliminary investigations and may process the data".[389]

Regarding *ex-ante* considerations, the new legislative provisions contain many of the *ex-ante* conditions recommended by the UN and other international stakeholders. Some of these were noted as improvements on the previous legislative provisions by the Venice Commission.[390] More specifically:

- Practices governed by Article 19 §1 require **prior authorisation by a district court**, generally courts of second instance. The process for authorisation is complicated. It is a process that requires input from three actors: a high-ranking police officer needs permission from the prosecutor to request authorisation from the court. However, under urgent circumstances (i.e. the risk of the loss of evidence), law enforcement may undertake such practices without prior consent. In such cases, consent must be granted by the district court within five days or the practices must be suspended and the data destroyed. In its criticism, the Venice Commission stated that, although the Polish authorities assured otherwise, the legal provisions could be interpreted to allow the short-term use of these practices by law enforcement (i.e. within the five-day limit) free from judicial control.[391] Therefore, it urges a reconsideration of this provision.
- Article 19 §7 stipulates the **details required within a law enforcement request to a district court for an operational control order**. Key points include:
    - **Point ii:** calls for the inclusion of a "description of the crime, stating, if possible, its legal qualification";
    - **Point iii:** calls for law enforcement to justify the necessity of the operational control to be performed, including an assessment of other means;
    - **Point iv:** calls for the inclusion of "personal data or other data facilitating unambiguous determination of the entity or object subject to operational control, stating the place or procedure for undertaking the control". Although the term 'object' is not defined, the Venice Commission considers that the "unambiguous determination" ensures that judicially authorised operational control practices are appropriately targeted; and
    - **Point v:** calls for details on the "objective, time and type of operational control referred to in Paragraph 6".

  Alongside such a request, law enforcement agencies are required to provide materials justifying the action. However, academic experts have suggested that the obligation to submit supporting materials (and not all materials) renders substantive control incomplete. What follows is a situation where approximately 94% of all requests have been authorised, and some courts have authorised 100% of requests.[392]
- Related to point v, above, the duration of an operational control practice is **limited to three months** (Article 19 §8). However, the "district court may, upon written request of the Police Commander in Chief or the Voivodship Police Commander, following written consent of the competent prosecutor" request subsequent periods of three months up to a **maximum of 18 months**[393] (Article 19 §9). Furthermore, Article 19 §12 states that

[389] *Id.,* Article 14 §4.

[390] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016, p. 8.

[391] *Id.,* p. 24, paragraph 93.

[392] Malgorzata Tomkiewicz, 'Podsluchy operacyjne w orzecznictwie sadowym' [Extra-judicial eavesdropping in case law] (2015) *Prokuratura i Prawo* 4, 153-171.

[393] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016, p. 8.

operational control practices must finish without delay, if the reasons for them cease to exist. However, the Council of Europe's Venice Commission criticises the Act's provisions, stating that the maximum length of operational control is "quite long".[394]

- Related to point ii, above, Article 19 §1 provides a **list of crimes** for which operational control is permitted.[395] This list is criticised by the Venice Commission as being "quite broad"[396] as it can theoretically be used for relatively minor criminal offences, if they fall within the broader fields mentioned (e.g. drug-related offences). In these instances, the practical application of the principle of proportionality should prevent the court from ordering such measures for minor criminal offences.
- An additional condition that has received criticism is included in Article 19 §15. This article stipulates that the collection of communications data protected by professional privilege (e.g. lawyer–client privilege) must be destroyed or its use must be limited. However, the Venice Commission highlights that the Act does not specifically prohibit the use of operational control on the communications of lawyers, stating that these provisions are insufficient. It further explains, stating that law enforcement collection of protected communications data (even if those data are inadmissible and destroyed) may lead to: i) the discovery of other inculpatory evidence – i.e. the 'fruit of the poisonous tree'[397]; and ii) law enforcement gaining a tactical advantage and undermining the trust between the defence lawyer and the accused.[398]

As mentioned above, the conditions included in the Polish Act on Police relate solely to law enforcement use of operational control for **preliminary investigations**. For criminal investigations, more restricted operational control capabilities are permitted and are governed by Articles 237 and 241 of the Polish Code of Criminal Procedure. These provisions relate specifically to surveillance and recording of phone conversations (Article 237) and other forms of communication, including e-mail (Article 241). Article 237 §1 stipulates that law enforcement must obtain authorisation from the court (or, in urgent circumstances, the prosecutor with subsequent court authorisation §2); §3 restricts the crimes for which such interception is permitted; §5 obliges the cooperation of telecommunication operators; and §8 stipulates that the evidence obtained through such an operation may only be used for the offence for which it was granted.

Provisions of the legal framework – *ex-post* considerations

In addition to the abovementioned *ex-ante* conditions, the Polish legal system has implemented a limited range of *ex-post* mechanisms for the supervision and oversight of operational control practices.

The primary means by which Polish legislation provides *ex-post* supervision and oversight is through **Article 19 §22 of the Act on Police**. This article states that "the Minister competent for internal affairs shall provide the lower (Sejm) and upper (Senat) chambers of the Parliament with information"[399] about operational control annually. In addition, as per

---

[394] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016, p. 23.

[395] For a full list, please see Council of Europe translation of article 19 §1 here: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)036-e.

[396] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016, p. 13.

[397] *Id.,* p. 21. The theory of the "fruit of the poisonous tree" proclaims that evidence, obtained as a result of information which had been obtained in breach of law, should also be declared inadmissible. For a detailed analysis of this theory see the ECtHR case Gäfgen v. Germany [GC], no. 22978/05, ECHR 2010.

[398] *Id*., pp. 21-22.

[399] Polish Act on the Police of 6 April 1990. Article 19 §22. Translation provided by the Council of Europe.

Article 19 §16a and 16b, the Police Commander in Chief is required to keep a "central register of requests and orders concerning operational control run by the Police authorities".[400]

Although these mechanisms provide transparency and accountability at a macro level, the Venice Commission determined that they "cannot replace the oversight of specific surveillance operations by an independent body".[401] This type of oversight and supervision does not currently exist in the Polish legal framework. There is no requirement to notify targets of operational control practices and no independent review in any cases of operational control.[402]

The Venice Commission further states that, in theory, an accused may be able to challenge the lawfulness of an operational control practice within his/her criminal proceedings. However, it goes on to raise a range of issues with the current legal provisions in Poland in this regard. Firstly, such a review of operational control would not allow a defendant (or an affected third party) to seek compensation for such unlawful operational control. Secondly, details of operational control practices and subsequent materials are often treated as secret in Poland, meaning that such details may not be disclosed to the defence. Thirdly, such a remedy would only be possible in a fraction of cases, given that such information may only be disclosed during criminal proceedings.[403]

Fundamental rights considerations

Beyond the abovementioned conditions, which provide for some of the most important fundamental rights safeguards, the respect for fundamental rights is specifically discussed in Polish legislation. For example, Article 14 §3 of the Act of Police states that "in the course of performing official duties, police officers shall be obliged to respect human dignity, as well as observe and protect human rights".[404]

Among the *ex-ante* and *ex-post* conditions, key fundamental rights safeguards (using the provisions set out by the judgement of Saravai v Germany as a baseline) include limiting the use of operational control to crimes of a certain gravity; ensuring the operational control practices are targeted; limiting the duration of operational control practices; and detailing cases where the results of operational control must be destroyed.

However, as mentioned above, the Venice Commission has criticised the list of crimes included in Polish legislation, the maximum duration of operational control and the provisions related to destroying data.[405] In addition, no provisions are included for the handling of data obtained and the precautions to be taken when communicating such data. This suggests that Poland faces fundamental rights challenges if the legislative provisions stipulated above remain in their current composition.

---

[400] Polish Act on the Police of 6 April 1990. *Article 19 §16a and 16b.*

[401] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016, pp. 27-28.

[402] *Id*., pp. 27-28.

[403] *Id*., pp. 27-28.

[404] The Constitution of the Republic of Poland states the same as the European Convention on Human Rights, that intrusion of the state into citizens' privacy should be justified, and only a clearly defined legal framework can legitimise limitations of citizens' rights through determined methods of invigilation.

[405] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016.

Technical means used for hacking by law enforcement

Beyond the provisions stipulated in Article 19 §6 of the Act on Police (detailed above), information about the tools, techniques and methods used by law enforcement agencies to undertake hacking practices is **classified**.

Hacking practices by the security services

Poland currently has five security and intelligence services. These are the Internal Security Agency (ABW), the Foreign Intelligence Agency (AW), the Central Anti-Corruption Bureau (CBA), the Military Intelligence Service (SWW) and the Military Counterintelligence Service (SKW).

The key measures related to the hacking practices of the security and intelligence services are included in the Act of 10 June 2016 on anti-terrorist activities.

Beyond stipulating the same operational capabilities as those detailed above for law enforcement agencies, the legal provisions include the ability for the ABW to request that the court order denial of access to IT and communications systems.[406] Furthermore, the legislative provisions call on the ABW to undertake security evaluations, allowing them to access data from all government agencies and private companies that provide critical infrastructure services.[407]

However, the activities of the security and intelligence services have received criticism. Amnesty International, for example, stated that this counterterrorism bill "consolidates sweeping powers, including enhanced surveillance capacity […] with no independent oversight mechanism".[408] Furthermore, Amnesty International criticised the use of a fast-track process for acceptance of the bill and the lack of consultation.

[406] Act of 10 June 2016 on anti-terrorist activities and on the amendments to other acts. Article 32. Unofficial translation accessed on 14.02.17 at: http://www.legislationline.org/topics/country/10/topic/5.

[407] Amnesty International. 2016. Poland: Counter-terrorism bill would give security service unchecked power. Public Statement. EUR 37/4263/2016.

[408] *Id.*

United Kingdom Country Report

Completed with the support of Dr. Paul Bernal, Lecturer in Information Technology, Intellectual Property and Media Law, UEA School of Law; Javier Ruiz Diaz, Policy Director, Open Rights Group; and Graham Smith, Partner, Bird and Bird.

Legal framework and context

Lawful hacking is labelled as 'equipment interference' in the UK, and is primarily recognised as the process of the national law enforcement (and other intelligence services) obtaining data from devices by interfering with the associated electronic equipment.[409] It "encompasses a wide range of activity, from remote access to computers to covertly downloading the contents of a mobile phone during a search".[410] Equipment interference is deemed as a necessity by the government when attempting to gain intelligence that may otherwise be inaccessible due to encryption in national security and serious crime investigations.[411]

The legal framework for hacking by the UK's law enforcement agencies and intelligence services is outlined in Part 5 (Equipment Interference)[412] of the Investigatory Powers Act (IPA),[413] which came into effect in November 2016. The IPA is accompanied by six Codes of Practice that provide the corresponding operational details and judicial oversight arrangements of the powers contained within the Bill.[414] A draft Equipment Interference Code of Practice[415] (EICP) was published in August 2016 and includes legal guidance for law enforcement agencies and intelligence services wishing to conduct lawful hacking. According to the IPA, the National Law Enforcement consists of the following groups of officers[416]:

1. Officers in a Police Force;
2. A National Crime Agency (NCA) Officer working in collaboration with the police force;
3. An immigration officer;
4. An officer of Revenue and Customs;
5. A designated Customs official; and
6. An officer of the Competition and Markets Authority.

However, it is important to note that the EICP and the IPA only legislate for hacking with the purpose of obtaining communications, equipment data or other information, as opposed to, for example, hacking to disrupt a system.[417] Any other forms of hacking by the national law enforcement falls under the category of 'property interference', and is governed by Part 3 of the Police Act 1997 ('the 1997 Act').[418] For the purpose of this case study, 'hacking by law enforcement' will refer to any type of equipment interference that is conducted in accordance with the IPA.

EICP defines equipment as anything producing "electromagnetic, acoustic or other emissions" and any device capable of being used in connection with such equipment.[419] This includes internet-enabled devices such as laptops and mobile phones, as well as storage devices and

[409] Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny (2016).
[410] *Id.*, p. 23.
[411] Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny (2016).
[412] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference.
[413] Investigatory Powers Act 2016. Chapter 25.
[414] Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny (2016).
[415] Equipment Interference DRAFT Code of Practice, Autumn 2016.
[416] Investigatory Powers Act 2016 (c. **25**) Schedule 6 – Issue of warrants under section 10 etc: table.
[417] Equipment Interference DRAFT Code of Practice, Autumn 2016, *Scope and Definitions.*
[418] Police Act 1997. C. 50 Part III Authorisation of Action in Respect of Property.
[419] Equipment Interference DRAFT Code of Practice, Autumn 2016, *Scope and Definitions,* p. 3.

cables.[420] Equipment data comprises two types of data: i) **systems data** are data associated with the communications or information being acquired that allow it to function, such as the version of a software operating system or router configurations; ii) **identifying data** are data that can be used to identify a person, event, location or item, or any information that doesn't facilitate the functioning of a service.[421] Any hacking that unlawfully accesses this information or interferes with the functioning of 'equipment' commits an offence under the Computer Misuse Act 1990.[422]

Provisions of the legal framework – *ex-ante* considerations

The IPA was introduced as a result of the findings of the Independent Reviewer of Terrorism Legislation, David Anderson QC, who was asked to "review the operation and regulation of investigatory powers"[423] available to the Government. This review was a concession of the passing of the Data Retention and Investigatory Powers Act 2014,[424] which enabled the UK law enforcement and security and intelligence agencies to continue to access telecommunications data in criminal investigations.

The report summarised that, whilst the Government had a lot of strong and largely necessary interception powers, they were enshrined in more than 65 different acts of parliament, with varying levels of appropriate protection given to innocent people who might be affected by those powers.[425] David Anderson QC concluded that the difficulty in understanding the powers effectively and the lack of associated safeguards made the legal framework "undemocratic, unnecessary and – in the long run – intolerable".[426] It has also been suggested that the national law enforcement stretched the laws to the limit; using them in ways that were not originally intended but were justified utilising vague and outdated legislative provisions.[427] Therefore, the independent review recommended "bringing those powers together into one place, into one act of parliament, which can be properly debated, easily understood and which applies proper safeguards onto the exercise of those powers".[428]

In response to Mr Anderson's report, the UK Government published a draft Investigatory Powers Bill[429] in November 2015, with a final version passed as law in November 2016 after various parliamentary debates and iterations of the Bill.[430] The IPA sets out the following objectives[431]:

1. To combine the powers available to law enforcement and the security and intelligence agencies in obtaining communications and communications data with appropriate safeguards, and present them in a clear and understandable manner;
2. To radically overhaul the authorisation of these powers and the necessary oversight required, which includes the creation of an Investigatory Powers Commissioner (IPC) position; and

[420] Equipment Interference DRAFT Code of Practice, Autumn 2016, *Scope and Definitions,* p. 3.
[421] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference, p. 79.
[422] Computer Misuse Act 1990 c. 18 Computer misuse offences.
[423] Data Retention and Investigatory Powers Act 2014 s7.
[424] Data Retention and Investigatory Powers Act 2014.
[425] A Question of Trust. Report of the Investigatory Powers *Review* by David Anderson Q.C. Independent Reviewer of Terrorism Legislation June 2015.
[426] *Id*., p. 8.
[427] Bernal, P. 2017. Expert interview conducted for this study.
[428] Interview with David Anderson QC, June 2015. *Surveillance powers: New law needed, says terror watchdog.*
[429] Draft Investigatory Powers Bill, November 2015.
[430] See e.g. Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny (2016).
[431] *Id*., p. 5.

3. To ensure the powers are fit for the digital age in response to the advances in communications technology.

In order to engage in lawful hacking, the national law enforcement must be issued with a **targeted equipment interference warrant by the appropriate law enforcement chief**, and usually only if the purpose is to prevent or detect a 'serious crime'.[432] A serious crime is defined as "an offence for which a person […] could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or (b) the conduct involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose".[433] However, officers in a police force or an NCA officer colluding with a police force may also be issued with a warrant "for the purpose of preventing death or any injury or damage to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health",[434] which is reported to usually relate to the location of vulnerable individuals.[435] In all cases, there must be a British Islands connection, meaning that at least some of the conduct, equipment interference or information must be due to occur in the British Islands at some point.[436] Furthermore, the law enforcement chief must deem the actions outlined in the **warrant to be necessary to the investigation and proportionate to the outcome**.[437] This means that: the scale of the intrusion must be weighed against the benefits of achieving the desired results of the investigation; the method should be the least intrusive means possible; and reasonable alternatives should be considered.[438] The Equipment Interference Code of Practice states that "[no] interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means".[439]

Usually, a targeted equipment interference **warrant must also be approved by a Judicial Commissioner (known as a double-lock authorisation safeguard[440])** before it can be issued. However, if the law enforcement chief considers the case to be urgent, this approval can be delayed.[441] The Judicial Commissioner must still authorise the warrant before the end of 'the relevant period' (within three working days of the warrant being issued).[442] If the Judicial Commissioner disagrees with the issuing of the urgent warrant, the Commissioner can cancel it and order the retrieval of any equipment used for interference. Alternatively, if the relevant law enforcement chief is not available in an urgent case, an appropriate delegate may issue a targeted equipment interference warrant.[443]

The EICP states that **actions outlined in the warrant must also avoid collateral intrusion**, wherever possible. Collateral intrusion refers to "obtaining private information about persons who are not subjects of the equipment interference activity",[444] and it is only permitted if it is absolutely necessary for the investigation. In these cases, proportionality

[432] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference.
[433] Investigatory Powers Act 2016 (c. **25**) *art 9* – Miscellaneous and general provisions Chapter 2 – General. p. 218.
[434] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference, p. 84.
[435] Equipment Interference DRAFT Code of Practice, Autumn 2016. Equipment interference warrants – general rules.
[436] Investigatory Powers Act 2016 (c. **25**) Part 1 – General privacy protections.
[437] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference.
[438] Equipment Interference DRAFT Code of Practice, Autumn 2016. Equipment interference warrants – general rules.
[439] *Id*., p. 22.
[440] Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny (2016).
[441] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference.
[442] *Id*.
[443] *Id*.
[444] Equipment Interference DRAFT Code of Practice, Autumn 2016. Targeted equipment interference warrants, p. 36.

must be applied as outlined above, and the proposed risks and mitigation actions must be defined in the warrant application.[445]

If the targeted equipment interference warrant involves equipment relating to multiple people, organisations or locations in the UK, it is sometimes referred to as a 'thematic warrant'.[446] There is no limit on the number of pieces of equipment to be outlined in a thematic warrant, meaning that little may be known about the individuals or organisations using them, although the warrant application must specify all the information that is known. [447] Therefore, a thematic warrant could be used when attempting to discover the hidden IP addresses of a certain website, for example.

The EICP also outlines considerations that must be assessed in a targeted equipment warrant if the hacking involves gaining confidential information, including confidential personal information, confidential information between a Member of Parliament and a constituent, and confidential journalistic information.[448] It states that warrants should clearly document the reasons for interfering with confidential information, and measures of necessity and proportionality should be considered.[449] Mitigation steps should be outlined in the warrant if there is a possibility of gaining confidential information, even if it is not the target of the investigation.[450] The same steps should be taken when retrieving or potentially retrieving communications subject to legal privilege, or those involving a high degree of privacy.[451] The IPA states that necessity in this case, as well as being pursuant to preventing a serious crime, death or injury, means that "the public interest in obtaining the information that would be obtained by the warrant outweighs the public interest in the confidentiality of items subject to legal privilege".[452] If a lawyer is being investigated through equipment interference and may have had access to communications subject to legal privilege, the warrant requires oversight from the Investigatory Powers Practitioner (see below).[453] However, legal privilege does not apply to communications or items held with the intention of furthering a criminal purpose.[454] Furthermore, a warrant that will interfere with communications of a member of the House of Parliament requires approval from the Secretary of State, who also needs authorisation from the Prime Minister.[455]

Other uses of equipment interference include facilitating covert surveillance. In this case, a separate surveillance warrant may be required or, alternatively, a combined warrant may be authorised, but the criteria for equipment interference and covert surveillance should be considered separately. In addition, a service warrant can be issued to any person or organisation, such as a network provider, that the law enforcement officer believes can assist in the equipment interference. In the case of telecommunications operators specifically (and presumably technology providers[456]), after receiving their own copy of the targeted

[445] *Id*.

[446] Equipment Interference DRAFT Code of Practice, Autumn 2016. *Targeted equipment interference warrants.*

[447] Equipment Interference DRAFT Code of Practice, Autumn 2016. *Targeted equipment interference warrants.*

[448] Equipment Interference DRAFT Code of Practice, Autumn 2016. *Handling of information, general safeguards and sensitive professions.*

[449] *Id.*

[450] *Id.*

[451] *Id.*

[452] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference.

[453] Equipment Interference DRAFT Code of Practice, Autumn 2016. Handling of information, general safeguards and sensitive professions.

[454] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference.

[455] *Id.*

[456] Nyst, C. 2017. Expert interview conducted for this study.

equipment interference warrant, they must do all that is reasonably practicable to assist in the operation.[457]

The Code of Practice states that "material obtained through equipment interference may be used as evidence in criminal proceedings".[458] In these situations, national law enforcement should demonstrate how the evidence was obtained and the equipment interference agency should be able to demonstrate how the evidence at each stage and process has been recovered in order to ensure the continuity and integrity of evidence.[459]

Provisions of the legal framework – *ex-post* considerations

The Investigatory Powers Commissioner is appointed by the Prime Minister, and is an additional layer of judicial oversight. The role of the Investigatory Powers Commissioner is to "ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny",[460] including reviewing all cases of equipment interference. Any dispute or complaint surrounding equipment interference – for example, a human rights claim – is considered by the Investigatory Powers Tribunal (IPT). The IPT is independent of the government and consists of members of the judiciary and "senior members of the legal profession".[461]

In addition, warrants must be reviewed to assess whether the hacking practice is still being completed in accordance with the agreed procedure – the point at which a warrant is reviewed is determined when it is issued. Any changes to the electronic interference that have not been specified in the procedure of the issued warrant may require a new warrant application. Otherwise, an equipment interference warrant issued by a law enforcement chief is valid for six months from the day it was issued, unless it is decided that it is necessary and appropriate to renew it (for another six months) – for example, to enable the removal of the means of equipment interference. In applying for a warrant renewal, details of the results obtained or an explanation of the failure to obtain them up until that point must be included. Warrants can also be modified by the law enforcement chief – for example, to remove or add a name or update the equipment description. The process of moderating a warrant is the same as applying for one (using grounds, necessity, proportionality, judicial approval, etc.), including the procedure in urgent cases. A warrant is cancelled when the law enforcement chief deems it no longer necessary (or proportionate) to the investigation, but results of the warrant should be retained for at least three years.[462]

The IPA states that the law enforcement chief (and judicial commissioner) must be satisfied that the number of people to whom the material is disclosed and the extent to which the material is made available or copied (including the number of copies) must be kept to a minimum as deemed necessary. A person with access to the material may only disclose information if it is authorised by the warrant, judicial commissioner, or if it is to be used in legal proceedings or in any case otherwise specified. Any material obtained under a targeted interference warrant must be securely destroyed as soon as there are no longer grounds (it is not necessary) to keep it. If any material is retained that contains or identifies an item subject to legal privilege, the Investigatory Powers Commissioner must be informed as soon

[457] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference.

[458] Equipment Interference DRAFT Code of Practice, Autumn 2016. Handling of information, general safeguards and sensitive professions, p. 77.

[459] Equipment Interference DRAFT Code of Practice, Autumn 2016. Handling of information, general safeguards and sensitive professions.

[460] Equipment Interference DRAFT Code of Practice, Autumn 2016. Oversight, p. 92.

[461] *Id*.

[462] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference.

as is possible, and the need to retain the material must be reviewed at appropriate intervals.[463]

Fundamental rights considerations

The UK's Human Rights Act (1998) operates in accordance with the European Convention on Human Rights. Whilst some of these rights are absolute, others, including the right to respect for private and family life and the right to peaceful enjoyment of possessions – of particular relevance to lawful hacking – are 'qualified'.[464] This means that certain measures can be taken that allow the national law enforcement and intelligence services to lawfully encroach on these rights.[465] For equipment interference to be consistent with the Human Rights Act, it would have to be necessary to achieve the protection of national security or the prosecution of serious crime, proportionate to those objectives, and sufficiently regulated by law, including being accompanied by sufficient safeguards to prevent abuse.[466] The definitions and tests of necessity and proportionality have already been set out in the above section, with reference to the Investigatory Powers Act and Draft Code of Practice.

Technical means used for hacking by law enforcement

The UK's legal framework for equipment interference does not include any provisions on the technical means that can be used to achieve the objective of an equipment interference warrant. Furthermore, there is very little information that is publicly available regarding the tools that UK law enforcement use, as highlighted by the NCA's statement, "the NCA leads the law enforcement response to serious and organised criminality impacting the UK. However, to preserve operational effectiveness we do not routinely disclose details of specific tools or techniques deployed in addressing those threats."[467] Whether tools are developed in-house or bought 'off-the-shelf' is also unclear and, additionally, there is very little guidance regarding the reporting of zero-day vulnerabilities. This non-disclosure of information and non-specific nature of legislation regarding tools is reported to allow the law enforcement to keep their options open for the use of hacking.[468]

Hacking practices by the security services

The IPA and EICP also applies to the UK Security and Intelligence Services, where a warrant is only necessary if it is: i) in the interests of national security; ii) for the purpose of preventing or detecting serious crime or; iii) in the interests of the economic well-being of the UK, and in relation to the acts or intentions of individuals outside of the British Islands, relevant to the interests of national security.[469]

Furthermore, specific authorities are permitted to use equipment interference in different scenarios. Only the security service (rather than the SIS and GCHQ) is allowed to gain a targeted interception warrant to investigate lawful hacking within the British Islands, along with the national law enforcement.[470] Though the process and requirements of the warrants are the same (e.g. including necessity and proportionality and other safeguard measures), the security service must obtain authorisation from the Secretary of State as well as a judicial

[463] *Id*.
[464] Equipment Interference DRAFT Code of Practice, Autumn 2016. *Introduction*
[465] Equipment Interference DRAFT Code of Practice, Autumn 2016. *Introduction*
[466] Nyst, C. 2017. Expert interview conducted for this study.
[467] Cox, J. 2016. What the UK's Proposed Surveillance Law Means for Police Hacking. *Motherboard*
[468] Bernal, P. 2017. Expert interview conducted for this study.
[469] Equipment Interference DRAFT Code of Practice, Autumn 2016. Targeted equipment interference warrants.
[470] Equipment Interference DRAFT Code of Practice, Autumn 2016. Equipment interference warrants – general rules

commissioner.[471] Therefore, the SIS and GCHQ are only able to use equipment interference in cases outside of the British Islands[472] and, when there is no British Islands connection at all, they are able to operate in accordance with section 7 of the 1994 Intelligence Services Act. The procedures are reported to generally be similar to targeted equipment interference warrants, but the process is typically faster as there is less authorisation required.[473]

All of the intelligence services are also able to apply for 'bulk equipment interference' warrants, which involves lawful hacking overseas on a generally larger scale and when there are less details about the target.[474] The process for acquiring a warrant is the same as for the targeted equipment interference warrants, as is the disclosure of any information or materials to overseas authorities.[475] However, if the bulk interference warrant involves any communication with an individual on the British Islands, the intelligence agencies may also need a targeted examination warrant.[476]

With regard to the actual use of hacking in practice, there is a high degree of secrecy surrounding the tools used by intelligence and secret services.[477] However, it is understood that GCHQ are given the biggest share of the intelligence budget and, as one of their explicit functions is to monitor or interfere with equipment in order to gain information in the interests of national security, it is therefore likely that they host the main technical abilities within the UK.[478] Furthermore, there is also good reason to believe that they have shared hacking capabilities with the NSA in the US, as highlighted in reports of the leaked documents from former NSA contractor Edward Snowden.[479] Reports suggest that GCHQ "appears to have played an integral role in helping to develop the implants tactic".[480]

Implant tactics include using social media sites such as Facebook or sending spam phishing emails to inject malware.[481] This malware can then be used to, for example, exfiltrate files from hard drives, reveal anonymised computer locations and computer browsing patterns, covertly record audio via a computer's microphone or take snapshots through its webcam.[482] Furthermore, whilst previously NSA deployed implants "for a few hundred hard-to-reach targets", a more recent, automated system (TURBINE) "allows the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually".[483] Statements also point to the importance of NSA sharing its capabilities with GCHQ, as quoted by the Director General of the Office for Security and Counter Terrorism at the Home Office, "In simple terms, the US can provide the UK with intelligence that the UK with its far more limited resources could not realistically obtain by itself."[484]

Furthermore, reports point to evidence of GCHQ using hacking malware to infiltrate mobile phones. This malware enabled the (covert) recording of conversations, identification of the

---

[471] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference

[472] Equipment Interference DRAFT Code of Practice, Autumn 2016. Equipment interference warrants – general rules

[473] Intelligence Services Act 1994. Section 7. Authorisation of acts outside the British Islands.

[474] Equipment Interference DRAFT Code of Practice, Autumn 2016. Bulk equipment interference warrants.

[475] Investigatory Powers Act 2016 (c. **25**) Part 6 – Bulk warrants Chapter 3 – Bulk equipment interference warrants.

[476] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference.

[477] Bernal, P. 2017. Expert interview conducted for this study.

[478] Ruiz, J. 2017. Expert interview conducted for this study.

[479] Gallagher, R. & Greenwald, G. 2014. How the NSA Plans to Infect 'Millions' of Computers with Malware. *The Intercept*.

[480] *Id.*

[481] *Id.*

[482] *Id.*

[483] *Id.*

[484] Statement of Charles Farr. 2014. Case No. IPT/13/92/CH.

user's location, and the retrieval of content.[485] However, in commenting on its involvement in hacking, GCHQ just stated that "all of GCHQ's work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorized, necessary and proportionate, and that there is rigorous oversight".[486]

[485] The Defendant's Conduct (16). Investigatory Powers Tribunal between Privacy International and (1) Secretary of State for Foreign and Common Wealth Affairs (2) Government Communication Headquarters.

[486] Gallagher, R. & Greenwald, G. 2014. How the NSA Plans to Infect 'Millions' of Computers with Malware. *The Intercept.*

APPENDIX 2: NON-EU COUNTRY REPORTS

Australia Country Report

Completed with the support of Dr. Adam Molnar, Lecturer in Criminology, Deakin University.

Legal framework and context

There is **no specific legal framework for the use of hacking by law enforcement** in Australia, and the legislation used to govern it has also not been publicly referenced.[487] However, whilst there is no legislation that mentions hacking by law enforcement specifically, inferences can and have been made regarding the most relevant Acts,[488] as highlighted below.

The **Telecommunications (Interception and Access) Act 1979**[489] (TIA) is the main framework for law enforcement to access communications that pass through telecommunications infrastructure. It has been amended at various stages since its inception so that it is now believed to be used to authorise hacking by law enforcement for the purpose of gaining access to communications.[490]

The **Surveillance Devices Act 2004 (SDA)**[491] presents the legal framework "for law enforcement officers to obtain warrants, emergency authorisations and tracking device authorisations for the installation and use of surveillance devices".[492] A data surveillance device is defined as "any device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer",[493] and a computer is defined as "any electronic device for storing or processing information".[494] Warrants cover the "installation, use, maintenance and retrieval of enhancement equipment in relation to the surveillance device".[495] It is therefore likely that – although it is not specifically specified – the SDA includes the use of hacking by law enforcement to permit surveillance on digital devices such as laptops, mobile phones, routers and other electronic devices.[496]

Provisions of the legal framework – *ex-ante* considerations

In order to access communications lawfully (i.e. through the TIA), a member of Australian law enforcement, which includes bodies such as the Australian Federal Police, Australian Crime Commission, the Police Force of a state, etc., must apply for a warrant under Part 2.5 of the TIA.[497] Through an affidavit, the application must set out the context for the investigation and the period for which the warrant would be in force, including why that period is necessary.[498] The application can either be made for a 'telecommunications service

---

[487] Molnar, A. 2017. Expert interview conducted for this study.

[488] *Id.*

[489] Telecommunications (Interception and Access) Act 1979. *Commonwealth Consolidated Acts.*

[490] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). Telecommunications (Interception and Access) Act 1979, CNOs, and counter-law. *Computer network operations and 'rule-with-law' in Australia.*

[491] Surveillance Devices Act 2004. *Commonwealth Consolidated Acts.*

[492] *Id.,* Sect 3 – Purposes.

[493] Surveillance Devices Act 2004. Sect 6 – Definitions. *Commonwealth Consolidated Acts.*

[494] *Id.*

[495] Surveillance Devices Act 2004. Sect 18 – What a surveillance device warrant authorises. *Commonwealth Consolidated Acts.*

[496] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). The Surveillance Devices Act 2004, CNOs, and counter-law. *Computer network operations and 'rule-with-law' in Australia.*

[497] Telecommunications (Interception and Access) Act 1979. Part 2.5 – Warrants Authorising Agencies to Intercept Telecommunications. *Commonwealth Consolidated Acts.*

[498] Telecommunications (Interception and Access) Act 1979. Sect 42. Affidavit to accompany written application. *Commonwealth Consolidated Acts*

warrant'[499] if the target individual is unknown, or for a 'named person warrant',[500] which must specify "details (to the extent these are known to the chief officer) sufficient to identify the telecommunications services the person is using, or is likely to use".[501] The warrant may be issued by a judge or member of the Administrative Appeals Tribunal (AAT)[502] and only if:

a. "There are reasonable grounds for suspecting that a particular person is using, or is likely to use, the service"[503]; and

b. The information gained by the warrant would "assist in connection with the investigation by the agency of a serious offence, or serious offences, in which:

   i. the particular person is involved; or

   ii. another person is involved with whom the particular person is likely to communicate using the service."[504]

Additionally, the judge or AAT member can only issue a warrant if all means of identifying the telecommunications service have been exhausted, and it is the only possible method of intercepting the communications.[505] The grounds for the issuing of the warrant is of note because, unlike other countries' legislation, there does not need to be reasonable suspicion that the target individual has committed an offence; instead the information must just be deemed to be useful for the investigation. A warrant to investigate a third party is valid up to 45 days from the date it is issued; otherwise, a warrant is valid for up to 90 days.[506]

Law enforcement officers must apply for a surveillance device warrant, using the SDA, if they have reasonable grounds to believe an offence will be committed, and that a surveillance investigation is necessary to obtain evidence of the offence or the identity or location of the targets.[507] Some of the information that surveillance device warrants must contain includes: a description of the alleged offences; the surveillance devices to be used; the premises/object/name of the target (depending on the nature of the investigation) and; the desired period of the warrant.[508] The maximum duration of a warrant is 90 days,[509] and this also applies to extension warrants.[510] In urgent circumstances in which the law enforcement officers believe immediate action to be necessary, a warrant can be issued by an appropriate officer, although they must apply for approval from a judge or nominated AAT member within 48 hours.[511]

---

[499] Telecommunications (Interception and Access) Act 1979. Sect 9. Issue of named person warrants by Attorney-General. *Commonwealth Consolidated Acts.*

[500] Telecommunications (Interception and Access) Act 1979. Sect 9A. Issue of telecommunications service warrants by Attorney-General. *Commonwealth Consolidated Acts.*

[501] Telecommunications (Interception and Access) Act 1979. Sect 42. Affidavit to accompany written application. *Commonwealth Consolidated Acts.*

[502] Telecommunications (Interception and Access) Act 1979. Sect 46. Issue of telecommunications service warrant. *Commonwealth Consolidated Acts.*

[503] *Id.*

[504] *Id.*

[505] Telecommunications (Interception and Access) Act 1979. Sect 46. Issue of telecommunications service warrant. *Commonwealth Consolidated Acts.*

[506] Telecommunications (Interception and Access) Act 1979. Sect 49. Form and content of warrant. *Commonwealth Consolidated Acts.*

[507] Surveillance Devices Act 2004. Sect 14 – Application for surveillance device warrant. *Commonwealth Consolidated Acts.*

[508] Surveillance Devices Act 2004. Sect 17 – What must a surveillance device warrant contain? *Commonwealth Consolidated Acts.*

[509] *Id.*

[510] Surveillance Devices Act 2004. Sect 19 – Extension and variation of surveillance device warrant. *Commonwealth Consolidated Acts.*

[511] Surveillance Devices Act 2004. Part 3 – Emergency Authorisations. *Commonwealth Consolidated Acts*

A judge or nominated AAT member may issue a surveillance device warrant if they believe "that there are reasonable grounds for the suspicion founding the application for the warrant".[512] In order to determine whether the warrant can be issued, they must also have had access to the context of the warrant application, the extent to which privacy is likely to be affected and details of any alternative means of obtaining the desired information from the warrant.[513] The judge or AAT member may also revoke the warrant at any time if they feel it is no longer applicable.[514] In addition, extraterritorial warrants may be issued to law enforcement offers if the surveillance will be needed in a foreign country.[515] However, there must be evidence to show "that the surveillance has been agreed to by an appropriate consenting official of the foreign country".[516]

Provisions of the legal framework – *ex-post* considerations

Both the TIA and SDA have additional *ex-post* oversight mechanisms through the internal reviewing of warrants. In both cases, the details of any warrants must be retained and reported to the appropriate Minister,[517] who must produce an annual report that highlights the number, duration and effectiveness of the warrants in the given period.[518] Furthermore, in both the TIA and SDA, an Ombudsman is required to inspect data and details of warrants to ensure compliance with the Acts.[519] However, the legislation does not specify the need to include any details regarding the use of lawful hacking, so the level of *ex-post* judicial oversight in practice is unclear.

However, mechanisms of public oversight appear to be limited. It is reported that the Australian Government do not wish to reveal details of their ability to hack,[520] and interpretations of Freedom of Information laws suggest that they do not have to.[521] Section 37 of the Freedom of Information Act (1982) states that a document is exempt from disclosure if it would "disclose lawful methods or procedures for preventing, detecting, investigating, or dealing with matters arising out of, breaches or evasions of the law the disclosure of which would, or would be reasonably likely to, prejudice the effectiveness of those methods or procedures".[522] Furthermore, the Crimes Act (1914) states that the disclosure of any confidential information by an officer is an offence,[523] and it has been suggested that this could apply to details of lawful hacking abilities, including the reporting of any information about zero-day vulnerabilities.[524] It has been argued that "legislation that enhances the Australian secrecy regime and establishes anti-whistle-blower laws have

[512] Surveillance Devices Act 2004. Sect 16 – Determining the Application. *Commonwealth Consolidated Acts.*

[513] *Id.*

[514] Surveillance Devices Act 2004. Sect 20 – Revocation of surveillance device warrant. *Commonwealth Consolidated Acts.*

[515] Surveillance Devices Act 2004. Part 5 – Extraterritorial Operation of Warrant, *Commonwealth Consolidated Acts*.

[516] *Id.* Sect 42 – Extraterritorial operation of warrants.

[517] Telecommunications (Interception and Access) Act 1979. PART 2-8 – Reports about interceptions under parts 2-3 and 2-5 – Division 1 – Reports to the Minister, *Commonwealth Consolidated Acts;* Surveillance Devices Act (2004). Part 6- Compliance and Monitoring – Division 2 – Reporting and Record Keeping, *Commonwealth Consolidated Acts.*

[518] Telecommunications (Interception and Access) Act 1979. PART 2-8 – Reports about interceptions under parts 2-3 and 2-5 – Division 2 – Reports by the Minister, *Commonwealth Consolidated Acts; Id.*

[519] Telecommunications (Interception and Access) Act 1979. PART 2-7 – Keeping and inspection of interception records, *Commonwealth Consolidated Acts;* Surveillance Devices Act (2004). Part 6- Compliance and Monitoring – Division 3 – Inspections, *Commonwealth Consolidated Acts.*

[520] Molnar, A. 2017. Expert interview conducted for this study.

[521] *Id.*

[522] Freedom of Information Act 1982 – Sect 37, Documents affecting enforcement of law and protection of public safety. Commonwealth Consolidated Acts. (2) (b).

[523] Crimes Act 1914, Sect 70 – Disclosure of information by Commonwealth officers. Commonwealth Consolidated Acts.

[524] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). Democratic Safeguards, Secrecy, and counter-law. Computer network operations and 'rule-with-law' in Australia.

exacerbated constraints on public disclosure and debate surrounding government usage of CNOs (lawful hacking)."[525]

Fundamental rights considerations

"Australia does not have a formal bill of rights or a regional judicial body to adjudicate on human rights",[526] and it has been argued that measures such as proportionality cannot be appropriately tested.[527] This has been reflected in the criticism of the use of non-targeted hacking, where it has been claimed that an abuse of powers could give law enforcement agencies almost "an unrestrained limit"[528] in the reach of their hacking. For example, with regard to the ruling in the TIA that extends hacking to third party individuals if it is thought that they might be communicated with,[529] it has been highlighted that this could mean that the warrant could extend almost indefinitely, e.g. to anybody whose data passes through a mobile tower.[530] Similarly, the SDA also permits interference with third party individuals,[531] as well as extending the authorisation of surveillance to a 'system'[532] that is connected to the target device, and has therefore also been criticised as surpassing proportionality.[533] Furthermore, legislation of hacking for both the law enforcement and security services has been criticised as outdated in comparison to technological advances, which therefore removes clear boundaries for the application of hacking.[534] It has been argued that the expansion of definition of a 'computer' in the ASIO Act 1979[535] (see below), which allows the Security Intelligence Service to conduct non-targeted hacking on a large scale,[536] could potentially be interpreted as allowing the hacking of an entire "core internet infrastructure".[537]

Hacking practices by the security services

Section 25A of the Australian Security Intelligence Organisation Act 1979 outlines the process of the Australian Security Service gaining a 'computer access warrant',[538] and is likely the primary legislation that governs lawful hacking by the Security Service.[539] Although it does not specifically mention hacking, Section 25A authorises the use of a target computer, a

---

[525] *Id.,* p. 9.

[526] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). Democratic Safeguards, Secrecy, and counter-law. Computer network operations and 'rule-with-law' in Australia. p. 9.

[527] *Id.*

[528] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). Discussion. Computer network operations and 'rule-with-law' in Australia. p.11.

[529] Telecommunications (Interception and Access) Act 1979 Sect 46. Issue of telecommunications service warrant. Commonwealth Consolidated Acts.

[530] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). Telecommunications (Interception and Access) Act 1979, CNOs, and counter-law. Computer network operations and 'rule-with-law' in Australia.

[531] Surveillance Devices Act 2004. Sect 18– What a surveillance device warrant authorises. Commonwealth Consolidated Acts.

[532] *Id., 3 (f).*

[533] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). Telecommunications (Interception and Access) The Surveillance Devices Act 2004, CNOs, and counter-law. Computer network operations and 'rule-with-law' in Australia.

[534] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). Discussion. Computer network operations and 'rule-with-law' in Australia.

[535] Australian Security Intelligence Organisation Act 1979, Commonwealth Consolidated Acts.

[536] Australian Security Intelligence Organisation Act 1979 Sect 22 – Interpretation, Commonwealth Consolidated Acts.

[537] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). The ASIO Act, CNOs, and counter-law. Computer network operations and 'rule-with-law' in Australia, p. 6.

[538] Australian Security Intelligence Organisation Act 1979 Sect 25A – Computer access warrant, Commonwealth Consolidated Acts.

[539] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). The ASIO Act, CNOs, and counter-law. *Computer network operations and 'rule-with-law' in Australia.*

Commonwealth telecommunications facility, "any other electronic equipment; or a data storage device; for the purpose of obtaining access to data",[540] which includes altering data in the computer.[541] Furthermore, the definition of a computer has been expanded to include "one or more computers […] computer systems […] computer networks; or any combination of the above",[542] giving the intelligence services a large scope with which to conduct their hacking.

Computer access warrants are issued by the Attorney-General following a request from the Director-General of ASIO.[543] The Attorney-General must be satisfied that the warrant would "substantially assist the collection of intelligence […] that is important in relation to security",[544] and it must be specific, where possible.[545] The warrant does not authorise actions that will "cause any other material loss or damage to other persons lawfully using a computer"[546] (although the definition of material loss is not specified), but it does allow the access of a third party individual's data if 'necessary'.[547] Furthermore, the ASIO may be issued with computer warrants for the purpose of gaining foreign intelligence if the "issuing Minister (Attorney-General) is satisfied, on the basis of advice received from the Defence Minister or the Foreign Affairs Minister, that the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being".[548]

Technical means used for hacking by law enforcement

In 2016, The Australian Cyber Security Centre (ASC) was given a large amount of funds to improve the security of Australian communications infrastructure.[549] The ASC is known to share intelligence analysts from a variety of intelligence and law enforcement bodies.[550] One of these intelligence bodies is the Australian Signals Directorate (ASD), who are known to possess hacking proficiencies.[551] As the ASD are able to provide assistance to law enforcement agencies,[552] and there is a growing general sense of blurred boundaries between various intelligence and law enforcement bodies anyway,[553] it is difficult to identify who uses what tools in practice, which is compounded by the fact that the Australian government does not wish to reveal details of its hacking capabilities.[554]

---

[540] Australian Security Intelligence Organisation Act 1979 Sect 25A – Computer access warrant, *Commonwealth Consolidated Acts.*

[541] *Id.*

[542] Australian Security Intelligence Organisation Act 1979 Sect 22 – Interpretation, *Commonwealth Consolidated Acts.*

[543] Australian Security Intelligence Organisation Act 1979 Sect 25A – Computer access warrant, *Commonwealth Consolidated Acts.*

[544] *Id.*

[545] *Id.*

[546] *Id.*

[547] *Id.*

[548] Australian Security Intelligence Organisation Act 1979 Sect 27A – Warrants for the performance of functions under paragraph 17 (1) (e), *Commonwealth Consolidated Acts.*

[549] Coyne, A. 2016. Govt to spend $230m on cyber security strategy. *Itnews.*

[550] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). The ASIO Act, CNOs, and counter-law. *Computer network operations and 'rule-with-law' in Australia.*

[551] *Id.*

[552] Australian Security Intelligence Organisation Act 1979 Sect 13 – Co-operation with other authorities in connection with performance of agency's own functions, *Commonwealth Consolidated Acts.*

[553] Bowling, B., & Ross, J. 2006. The Serious and Organised Crime Agency: Should we be afraid? *Criminal Law Review, December,* 1019-1034.

[554] Molnar, A. 2017. Expert interview conducted for this study.

Therefore, any details about tools or methods used by law enforcement and security agencies have to be deductively inferred from court cases or online reports and leaks.[555] For example, when emails from Hacking Team were released, it was revealed that the Australian Federal Police (AFP) had been a client.[556] Furthermore, other law enforcement bodies and intelligence/security services, such as ASIO, had been in contact with Hacking Team, including one claiming the Australian Defence Force as its client.[557] The New South Wales (NSW) police also reportedly acquired licences from another hacking technology company, Gamma Group, specifically for their FinFisher spyware software.[558] In general, little is known about exactly what technologies are being sold and used.[559] However, reports such as the child pornography investigation[560] outlined earlier in the report offer some insight, such as the use of phishing attacks as highlighted in that case specifically. Furthermore, reports have suggested that the intelligence agencies are increasing their in-house development of zero-day exploits.[561] However, the number of successful findings that are shared with Australian law enforcement agencies is unknown, and it is believed that the various policing bodies are more likely to use off-the-shelf tools.[562]

[555] Molnar, A. 2017. Expert interview conducted for this study.

[556] Sveen, B. & Ockenden, W. 2015. Hacking Team: Australian Government agencies negotiating with notorious surveillance company, leaked emails show. *ABC News.*

[557] Duffy, C. & Main, L. 2015. Australian police and Defence Force used infamous Hacking Team, Wikileaks reveals

[558] Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). The ASIO Act, CNOs, and counter-law. *Computer network operations and 'rule-with-law' in Australia*

[559] *Id.*

[560] Cox, J. 2016. Australian Authorities Hacked Computers in the US. Motherboard

[561] Molnar, A. 2017. Expert interview conducted for this study.

[562] *Id.*

Israel Country Report

In the absence of specific legislation that defines, controls and regulates hacking by law enforcement agencies, the powers of law enforcement and security agencies in many third world and developing countries, including Israel, have grown largely unchecked.

The Israeli legal definition of 'computer' includes storage devices such as tablets, mobile phones, disks, external hard drives and encryption devices that make it harder in some cases to break some codes. Collectively these are commonly referred to as 'cyber systems'.

The lawful hacking of cyber systems is, perhaps, one of the most politically sensitive issues in Israel. It is a frontline defence against terrorist activities. Hence, it comes as little surprise that, particularly over recent years, national law enforcement agencies have been given greater powers to exercise lawful hacking. The Computers Act 1995 amends existing legislation to address the issue of digital evidence and, in 2007, the Communication Act was enacted to cover the accepted practice of obtaining information from internet-access providers; information that could be considered more personal than site content.

The use of hacking techniques by law enforcement agencies has repeatedly provoked human rights debates that centre on privacy and whether 'hacking by law enforcement' is actually lawful at all. Indeed, such hacking practices are only permitted in the most extreme cases yet, in practice, hacking orders are commonplace. This has given rise to criticisms of these practices. However, Israel has implemented periodic reporting requirements to parliament and to the attorney general.

Israeli laws pay exceptional attention to computer crime, data searches and sensitivity and data and system acquisition and seizure. These laws acknowledge and address hacking, information retrieval and the invasion of privacy. Computer resources are given special consideration during legal investigations and their seizure or interception and subsequent use in legal proceedings often involves balancing the rights of the suspect and third parties against law enforcement and security objectives.

In 2010, the Israeli government also afforded security and law enforcement agencies greater investigative powers, in relation to both physical and digital data. The primary aim was to tackle the terrorist use of the internet. Since 2010, security agencies have been able to secretly but lawfully search stored computer data.

Court orders that relate to cyber and physical computer systems and data give rise to significant challenges for Israeli law. In an interview Kobi Freedman stated that the word 'hacking' is not a legal term in Israel and that, instead, the executing authorities use the term 'legal penetration'. The latter legalises data collection for investigations and 'device-penetration' or hacking. Moreover, whilst computer hacking is only lawful when executed by warrant or court order and when conducted by an officer of the law during a search, there are questions about what actually constitutes lawful exercise of a hacking order.

Nemrod Kozlobscki states:

"The firm legal situation related to computer search does not give sufficient response and answer in relation to hacking computers. Legal provisions are lacking fundamental basic groundwork that must be found in the provisions governing the authority of conducting a search on an individual and it does not give sufficient guiding tools for law enforcement authorities and courts especially in relation to the implementations of those searches."[563]

Freedman states that:

[563] Kozlobscki, N. 2000. The Computer Legal Proceeding 54, p. 619.

"The authority gives officers the right to investigate and keep evidence track recording; every incident is treated specifically per suspect, per crime and per event."[564]

Indeed, there are many ways to mask criminal activity and evade detection, including encryption, the use of proxy servers and/or data streaming via secured networks. Often, information is transmitted and/or stored outside of the jurisdiction, which introduces an international dimension to the issue of lawful hacking since the legal frameworks that protect human rights can differ between jurisdictions and since international cyberspace has, in effect, its own laws and rules of conduct. Even when information is stored on a physical device within the jurisdiction, there is always a risk that it is mingled with highly personal information that bears no relation to the lawful search but that might be inadvertently seized or destroyed during the execution of a warrant.

There must be a balance struck between the protection of public interest or national security and the rights of the suspect or third parties. Handling of computer data must be logged because of the possibility of data being altered, lost or corrupted. This is particularly important when such data are to be relied upon as evidence and to ensure that any individual's rights to privacy are not compromised without legal justification.

In coming to a decision as to whether to authorise an order for hacking, the court must follow two rules. The first rule is checking whether hacking is necessary, in light of the circumstances and the evidence. In coming to a decision, the court must, therefore, undertake a detailed and documented review of the order requested by the police. The second rule requires that legislation be given by the courts in a way that takes into consideration the current state of art, namely the ever-changing world of computer-based technologies.

Executing an order to tackle cybercrime, as opposed to other forms of crime, requires that the possibility that computers and data can change hands very quickly and data can suddenly become inaccessible is taken into consideration. Thus, one person might have 'access' to the computer but the computer may be in another person's possession. It is also possible that access and control of data stored on the device differs and that the person who owns the computer is not the person in possession of it. Any of these people might be the suspect and any one of them may have exercisable or protected rights to the computer and/or data stored on it. One more definition, therefore, relates to the 'holder' of the computer sources, whose presence is required during the penetration, and the location or the place where the computer is found.

The court has the discretion to inform the suspect about an impending lawful hack. If the court determines this to be necessary, a police officer must be present when the suspect is informed. When the order is being executed, a detailed description of the computer must be documented. Details such as the type, characteristics, specification and manufacturer of the device, mode of communication between the recipient and suspect and service provider and service type are recorded. Once the order has been granted, the court has a legal obligation to provide the suspect with a detailed order that outlines the reasons why the order was granted, the order's volume and the conditions that must be satisfied during the execution of the order. If, however, the order is served on the 'service provider', the court can choose whether to inform the suspect about the impending investigation. The suspect is not supposed to be informed about the investigation against him to date when he gets the right of inspection of the suspected material after indictment.

An administrative order is only granted in exceptional circumstances, such as when there is a need for urgent action. In such circumstances, orders can be granted even though there is

[564] Freedman, K. 2017. Expert interview conducted for this study.

a potentially high risk of invading the privacy of the suspect. Such orders are generally only executed by high-ranking and qualified officers and then within a 24-hour timeframe.

Law enforcement and security agencies have powers that enable them to hack computers to determine details such as the whereabouts of computers, their users, possession and ownership and whether or not the computer is an administrative or private device. Other information that might be obtained prior to the issue of a court order includes details of service provision. In exercise of these powers, the authorities must document the details of the actions they have taken prior to obtaining a court order. Upon the subsequent granting of a hacking order, the court is required to identify the computer and give details of the hacking process, as well as set conditions that ensure hacking does not disproportionately impact upon the privacy of the suspect or third parties.

At times, the court is permitted to authorise a biphasic hacking strategy. For instance, when the court suspects that this is the only way to prevent a disproportionate invasion of the suspect's privacy, the court can limit the scope of the hack to specific computer materials. Once this hack has been executed, the order will contain provisions that assist subsequent hacking, if this is appropriate.

When an order is executed and the hack reveals that the suspected computer materials do not exist, a second order can authorise hacking of another of a suspect's computers, a server or a computer owned or in the possession of a third party or even a public computer. Any such order must protect the rights of third parties that are affected by the execution of the order.

If a police officer suspects a crime will be committed and that crime could endanger the lives or security of other people or of the public or if it could impact upon state security, the court can permit hacking into a computer without first granting a court order. Under such circumstances, computer hacking becomes a means to gather intelligence related to the suspected crime and bypasses investigative problems that could arise whilst waiting for a court order to be issued. In such cases, law enforcement officers who hold the rank of chief superintendent and above are authorised to hack a computer without a court order when immediate action is warranted, namely:

- When there is an imminent risk to life;
- The computer information sort is evidence of a crime and immediate hacking would prevent destruction of that evidence;
- The time of the legal order will not exceed 24 hours;
- The order should be a written one that details the identification of the person giving the order, a summary of information, and evidences justifying and permitting the action; and
- The officer is allowed to hack and copy the materials only and the viewing is permitted after the order has been provided.

The exercise of such powers is reviewed by the government's legal counsel, the recipient of the report on such orders.

There are cases where the computer is inaccessible because, for example, the network that incorporates the computer is a complex or if disconnecting the computer from the server or hacking into it might disrupt network service or impact other computers in the network. In such cases, data may be copied or the computer might be seized. Then the agent responsible will review the situation after hacking has taken place.

In general, lawful hacking should be conducted with witnesses present. Hacking without first informing the holder of computer material represents a significant violation of the holder's rights and, potentially, the rights of third parties as this denies them the opportunity to

witness the hack or authorise their own expert to be present. This will also be the case when the case is to pass to special security services that are authorised to hack without first seeking permission of the holder. Unauthorised and uninformed hacks are rare and generally limited to instances where there is a wider public interest and when the holder might alter or delete computer-based evidence or when a delay might result in a suspect being tipped off, with consequences for the investigation.

Generally, any computer files that are copied must be documented for administrative inspection. The hacking officer must identify himself, present the court order and indicate his or her authority to force compliance. Legally, the officer must inform the suspect about his or her rights. Any suspect who is not a suspected terrorist has the right to ask for his own computer specialist to be present before hacking commences.

If the computer's owner claims that he or she is not the only person permitted to have access to the computer materials, the officer must make reasonable efforts to ascertain and contact persons who have access to the computer materials. Any person who is served a hacking order can instruct an expert to act on his or her behalf.

There are times when law enforcement officers are unable to access encrypted computer files. In such circumstances, officers might request and be given password information by the suspect. A court can consider refusal to impart such information as sufficient evidence of wrongdoing. However, the fact that the suspect has provided password information does not provide a defence if incriminating materials are later found on the device.

When a request for a hacking order is presented to the court, the court will determine the nature of the order that is appropriate for the circumstances at hand. In coming to a decision, the court will weigh invasion of privacy and the suspect's other rights against the intended purpose of the hack. The issue of privacy is less important when the computer is already designated for public use. In such circumstances, acquiring a court order prior to hacking is not essential.

When the court feels it necessary to issue an order, it may issue a 'finding order' or allow computer files to be retrieved, copied and stored, or seizure of the computer itself.

There is generally a provision that requires that the suspect is given notice of the hacking order before it is executed. Courts generally prefer computers to be seized and specific files to be copied or recovered from the device when the suspect does not own the computer. There is some reluctance to issue orders that allow files and data to be intercepted or to issue orders that do not specify the nature of material that can be seized or copied.

According to Kobi Freedman, where there is a terror risk, Israeli legislation allows the police to tap telephones indefinitely if procedure is followed and documented. The officer himself should examine the act when the notion of necessity comes into the picture.

There is some reluctance to issue orders that allow files and data to be intercepted or to issue orders that do not specify the nature of material that can be seized or copied. When interception is permitted without the suspect's knowledge, however, it is not considered to be a human rights violation. Freedman refers to the 'fruit of the poisoned tree' law, where evidence can be admitted even though the suspect was not aware he was the subject of surveillance. This is because the main concern for the authorities is data collection and this subserviates the individual's right to privacy. When asked about the new legislative proposals for lawful hacking by Israeli authorities, Freedman drew attention to the current disparity within the Israeli legal system when it applies to military and civil matters.

United States Country Report

Completed with the support of Nate Cardozo, Senior Staff Attorney, Electronic Frontier Foundation; Kevin Bankston, Director of New America's Open Technology Institute; Ross Schulman, Senior Policy Counsel at New America's Open Technology Institute; Melissa Hathaway, Senior Advisor, Belfer Center for Science and International Affairs; and Chris Soghoian, Principal Technologist, ACLU.

Legal framework and context

There is no detailed piece of US legislation specifically regulating the use of hacking by law enforcement.[565] Whilst federal statutes such as Part I of the Electronic Communications Act (ECPA) (1986)[566] – an expansion of the 'Wiretap Act' (1968)[567] – and the Stored Communications Act (SCA)[568] govern law enforcement surveillance of real-time and stored communications respectively, both statutes pre-date the use of government hacking.[569] Instead, although never expressing it as absolute policy,[570] law enforcement agencies have generally sought authorisation for the use of hacking in investigations in search and seizure warrants applied under Rule 41 of the Federal Rules of Criminal Procedure (Rule 41).[571] The recent amendments to Rule 41 in December 2016[572] appear to confirm it as the most relevant piece of US legislation by offering a procedure for law enforcement agencies to gain 'remote access' of data.[573] Previously, the grounds for issuing warrants in this respect were disputed by US Courts,[574] as demonstrated below.

The first publicly reported court case of Rule 41 being used as a legal framework for hacking occurred when a Myspace user made bomb threats to a high school in 2007.[575] Although the exact location of the culprit was unknown,[576] the venue of the threatened act of domestic terrorism was released, thus relating to an exception of this requirement.[577] A search warrant was issued which permitted the government to use lawful hacking to identify the individual and their location through a phishing email, although not to access the content of any electronic messages. Conversely, venue conditions of Rule 41 have also been used to deny warrants involving hacking. In a Texan district in 2013, a judge rejected the government's request for a search warrant to gather information in a fraud case through lawful hacking.[578] The judge determined that the warrant would not meet the territorial exceptions of Rule 41,

[565] Expert interview conducted for this study. 2017.

[566] 18 U.S.C. § 2510 – an expansion of the Wiretap Act to include digital communications

[567] Omnibus Crime Control and Safe Streets Act (1968), P.L. 90-351, 801, 82 Stat. 197, 212 – provides the US government with procedural regulations surrounding the interception of real-time telecommunications.

[568] 18 U.S.C. Chapter 121 §§ 2701–2712

[569] The first report of the US government possessing the capability to use remote hacking in an investigation was in 2001 – Thompson, R.M. (2016). Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Background on Amendment to Rule 41.

[570] Crump, C. (2017) Interview

[571] Thompson, R.M. (2016). Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Congressional Research Service

[572] FED. R. CRIM. P. 41.

[573] FED. R. CRIM. P. 41. (b) (6)

[574] Crump, C. (2017) Interview

[575] Any Computer Accessing Electronic Message(s) Directed to the Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Message(s) Delivered to that Account By the Government, No. 3:07-mj-05114-JPD (W.D. Wash. June 22, 2007).

[576] The issuing of a search warrant through Rule 41 usually required the venue of the target to be specified, barring certain exceptions – FED. R. CRIM. P. 41. (b) (1)

[577] The relevant exception being when activities of domestic or international terrorism for which an investigation was being carried out had affected that district – FED. R. CRIM. P. 41(b)(3)

[578] Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013).

as both the target device enabling the scheme and its location were unknown,[579] and the government could not adequately explain how they would find it.[580] The judge also stated that the implications of such an intrusive means of investigation presented a risk in targeting innocent computers.[581]

The increasing use of anonymising technologies allowing criminals to mask their IP using proxy addresses, and the use of large-scale attacks, such as botnets, where a network of computers are attacked in potentially multiple districts,[582] implied that rulings such as the above could be more common.[583] Therefore, the Department of Justice requested amendments to Rule 41 in order to expand their lawful hacking powers.[584] The proposed amendments were published for public comment in August 2014[585] and on 28 April 2016, the Supreme Court presented a proposal to Congress. The Rules Enabling Act[586] meant that, as Congress did not respond with enacted legislation, the proposed rule came into effect in December 2016. Rule 41 now specifically presents law enforcement with the ability to be granted search warrants to "use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or (B) […] the media are protected computers that have been damaged without authorization and are located in five or more districts."[587] It is too early to tell exactly how these amendments will impact the use of hacking by law enforcement agencies or whether they will be coupled with revisions of statutes such as the ECPA.[588]

Provisions of the legal framework – *ex-ante* considerations

US legislation does not vary procedurally according to different contexts surrounding the use of lawful hacking, such as the scale of the crime committed or the target of the hack.[589] Instead, the key requirement permitting the use of hacking as a lawful search in accordance with the Fourth Amendment and Rule 41 is 'probable cause'.[590] If a federal judge or magistrate deems there to be probable cause of a crime being committed, they are able to grant a search warrant for the use of hacking independent of the circumstances and the process follows the procedural laws outlined in Rule 41, including using any material uncovered by the hacking as evidence.[591]

The other requirement for issuing a warrant in line with the Fourth Amendment is 'particularity'[592] – i.e the officers must describe the target of the warrant. However, in cases of lawful hacking the aim is often to identify the device's location and/or owner, which makes describing the target with particularity difficult.[593] Therefore, 'anticipatory' warrants are often

[579] *Id*. at 758.
[580] Warrant. 958 F. Supp. 2d at 759.
[581] *Id*.
[582] FED. R. CRIM. P. 41. Committee Notes on Rules—2016 Amendment
[583] Thompson, R.M. (2016). Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. *Amendment Process*
[584] Memorandum, Department of Justice to Advisory Committee on Criminal Rules 2 (Sept. 18, 2013),
[585] Docket Folder, Proposed Amendments to the Federal Rules of Criminal Procedure
[586] 28 U.S.C. §2074
[587] FED. R. CRIM. P. 41(b)(6)
[588] Crump, C. (2017) Interview
[589] Expert interview conducted for this study. 2017.
[590] U.S. CONST. amend. IV
[591] Expert interview conducted for this study. 2017.
[592] Marron v. United States, 275 U.S. 192, 196 (1927)
[593] Mayer, J. (2016). Constitutional Malware. Stanford University, School of Engineering, Computer Science, Stanford, CA, United States

used to combat this issue.[594] Anticipatory warrants operate on the basis that particularity and probable cause requirements will be triggered if a predicted set of circumstances are confirmed.[595] In the case of lawful hacking, the government can "articulate a conditional set of facts to ensure a fair chance that their malware will be delivered, and when it is delivered, to a computer system that satisfies probable cause and particularity".[596] For example, if the law enforcement uses a watering hole attack on an illegal website by adding malware that will reveal a computer's identity, probable cause of an offence being committed and particularity of the target can be confirmed once a user visits the website. However, this can present safety issues, as highlighted in the section on human rights, below.

Details surrounding the method of hacking to be used are generally not required in the application for a search warrant.[597] For example, the details of normal search warrants (e.g. whether the government is planning to knock on the door or enter via the window) are not usually specified, and the same standards are applied to cases of lawful hacking.[598] Arguments have been made which highlight the potential implications in affecting innocent users, and these are discussed below.

As established earlier, the governmental approach seems to necessitate obtaining a search warrant in accordance with Rule 41 for the use of lawful hacking. This therefore requires prior authorisation from a magistrate or district judge, and the timeframe for executing a warrant is a maximum of 14 days from issuance.[599] As giving notice to the target is likely to defeat the purpose of the hacking,[600] the Government are likely to be entitled to seek 'delayed notice',[601] as has been the case in many wire-tap investigations.[602] However, the Government must eventually give notice, meaning lawful hacking is usually subject to ex-notice requirements.[603] The amendment to Rule 41 states that in cases of accessing electronically stored media, the Government must "make reasonable efforts to serve a copy of the warrant and receipt" and ensure service is "reasonably calculated to reach that person."[604] However, when the Government uses hacking to reveal the identity of a hidden computer, and they use an anticipatory warrant, they have generally been required to give conditional *ex-post* notice.[605] This means that they give notice only to the individuals for whom they have issued a court order and have therefore revealed the identity of.[606] In practice, they might have affected more individuals with the malware, but have not deemed them guilty and hence not revealed their identity, meaning they haven't given them *ex-post* notice of the malware on their computer.

---

[594] E.g United States v. Karo, 468 U.S. 705, 718 (1984)

[595] *Grubbs*, 547 U.S. at 96-97

[596] Mayer, J. (2016). Constitutional Malware. Stanford University, School of Engineering, Computer Science, Stanford, CA, United States, p. 59.

[597] Expert interview conducted for this study. 2017.

[598] *Id.*

[599] FED. R. CRIM. P. 41(e)(2)(A)

[600] Berger v. New York, 388 U.S. 41, 86 (1967)

[601] FED. R. CRIM. P. 41(f)(3)

[602] 18 U.S.C. § 2518(8)(d)

[603] Mayer, J. (2016). III Rules for Malware: (E) Notice. *Constitutional Malware.* Stanford University, School of Engineering, Computer Science, Stanford, CA, United States

[604] FED. R. CRIM. P. 41(f)(1)(c)

[605] Mayer, J. (2016). III Rules for Malware: (E) Notice. *Constitutional Malware.* Stanford University, School of Engineering, Computer Science, Stanford, CA, United States

[606] *Id*.

Provisions of the legal framework – *ex-post* considerations

Rule 41 states that the Government must return a "copy of the inventory to the magistrate judge designated on the warrant",[607] and that, for cases of lawful hacking, "the inventory may be limited to describing the physical storage media that were seized or copied".[608] This further shows that the law enforcement agency does not have to specify the method of hacking used, only what was taken. "The judge must, on request, give a copy of the inventory" to the target of the investigation.[609] As the nature of the hacking conducted in investigations is often withheld from judges, and court orders are often kept sealed in any case, the subject of lawful hacking by the US Government is considered a relatively secretive topic.[610] Much of the information on the topic is a result of government leaks or deductive research by journalists.[611] It is understood that national law enforcement does not reveal their techniques for fear of tipping off criminals and making the methods redundant.[612] However, this further raises the issue of accountability and transparency, and the lack of legislation instructing the actions of the Government if they find a zero-day exploit has been labelled as a security threat.[613]

Fundamental rights considerations

When lawful hacking requires a search warrant, it is automatically bound by the safeguards of 'probable cause' and 'particularity' routed in the Fourth Amendment to the US Constitution. However, because its use has been largely shrouded in secrecy,[614] courts are just beginning to grapple with how the constitution's protections apply to lawful hacking specifically, with no appeals courts ruling on it to date.[615] Moreover, there is no legislation specific to hacking by law enforcement outlining fundamental rights safeguards that must be implemented.[616] The recent changes to Rule 41 allowing judges to issue warrants when the target location is unknown have also been criticised for breaching the particularity element of the Fourth Amendment.[617] It has been argued that using techniques such as watering hole attacks and phishing attacks can lead to innocent parties being infected by malware. For example, a phishing email could be forwarded to other addresses, and there have been examples of individuals visiting websites subject to a watering hole attack for a valid, legal reason, e.g. research or journalism.[618]

The Wiretap Act (1968) implemented four core safeguards when intercepting real-time communications interceptions, effectively requiring a 'super-warrant' to be issued.[619] The safeguards require that[620]:

---

[607] FED. R. CRIM. P. 41(f)(D)

[608] FED. R. CRIM. P. 41(f)(B)

[609] FED. R. CRIM. P. 41(f)(B)

[610] Expert interview conducted for this study. 2017.

[611] *Id*.

[612] Mayer, J. (2016). Constitutional Malware. Stanford University, School of Engineering, Computer Science, Stanford, CA, United States.

[613] ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media (2016) II. Technological and Policy Concerns (C) Law enforcement agencies will increasingly need zero day exploits

[614] Crump, C. (2017). Interview.

[615] *Id.*

[616] Hathaway, M. 2017. Expert interview conducted for this study.

[617] Thompson, R.M. (2016). Issues Raised by Proposed Amendment to Rule 41 – Particularity of Search. *Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure.* Congressional Research Service

[618] *Id.*

[619] 388 U.S. 41, 58-60 (1967).

[620] 18 USC. § 258 (1)-(5)

1. Ordinary investigate techniques have been exhausted
2. The surveillance is limited (time-bound) to what is necessary for the investigation
3. Particularity in the desired communications to be intercepted
4. Minimisation of non-relevant communications.

Whilst courts have applied these safeguards to video surveillance,[621] there is nothing in the Rule 41 amendments regarding the process if the Government remotely accesses a device for real-time content, e.g. by activating a microphone or camera.[622] The Judicial Conferences Committee Note suggests resolving issues such as this on a case-by-case basis,[623] but court cases following the Berger doctrine have suggested that remotely accessing a computer's camera or microphone requires a super-warrant.[624] Furthermore, some courts have also necessitated super-warrants when the government has interrupted real-time content in the form of internet connectivity,[625] or remotely monitored key strokes or screen content whilst the target is typing or receiving communication.[626]

Technical means used for hacking by law enforcement

The first reported case of hacking by law enforcement was in 1999, when the FBI installed a Key Logger System to record what was typed into a suspect's computer.[627] Since then, the US government has used a range of methods to deliver malware remotely using 'network investigative techniques' (NITs).[628] Although the government rarely comments on their hacking capabilities, case summaries and reports have revealed some of the methods used:

- Phishing attacks – for example, in revealing the identity of the Myspace user who made bomb threats to a high school in 2007, highlighted earlier in this section.[629]
- Watering hole attacks – for example, 'Operation Torpedo' of 2012 attached an NIT to a child pornography site which collected IP addresses and other identifying information of users,[630] resulting in 14 individuals being brought to trial.[631]
- Activating microphones in certain electronic devices to covertly record conversations.[632]
- Accessing cameras in certain electronic devices to record covertly (including not turning on the light that usually signifies recording).[633]
- Installing a system that can monitor keystrokes[634] or record screen activity.[635]

---

[621] United States v. Cuevas-Sanchez, 821 F.2d 248, 250 (5th Cir. 1987).

[622] Thompson, R.M. (2016). Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Congressional Research Service

[623] supra note 57.

[624] Mayer, J. (2016). Constitutional Malware. Stanford University, School of Engineering, Computer Science, Stanford, CA, United States.

[625] .g., Joffe v. Google, 746 F.3d 920, 926-36 (9th Cir. 2013)

[626] Luis v. Zang, No. 1:11-cv-884, 2013 WL 811816, at *12-25 (S.D. Ohio, Mar. 5, 2013

[627] Quinlan, S. & Wilson, A. (2016). Hacking the Mob with Keyloggers. A Brief History of Law Enforcement Hacking in the United States.

[628] Quinlan, S. & Wilson, A. (2016). Hacking the Onion Router. A Brief History of Law Enforcement Hacking in the United States.

[629] Any Computer Accessing Electronic Message(s) Directed to the Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Message(s) Delivered to that Account By the Government, No. 3:07-mj-05114-JPD (W.D. Wash. June 22, 2007).

[630] See Kevin Poulsen, Visit the Wrong Website, and the FBI Could End up In Your Computer, WIRED (Aug. 5, 2014), available at https://www.wired.com/2014/08/operation_torpedo.

[631] Poulsen, supra note 22.

[632] See Jennifer Valentino-DeVries and Danny Yadron, FBI Taps Hacker Tactics To Spy on Suspects, WALL STREET JOURNAL (Aug. 3, 2013).

[633] See Timberg & Nakashima, supra note 18.

[634] United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

[635] United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *3 (D. Neb. Aug. 5, 2016).

- Installing software that can access files in the device.[636]

Within the law enforcement sphere, hacking is believed to be routinely carried out at local and state level but only in a basic form that requires little training, e.g by using a plug and play device.[637] More sophisticated hacking such as the use of remote access and 'forensic hacking' (access to a flagship device with advanced security capabilities) is generally only available to the FBI and, even then, only in more exceptional circumstances.[638] However, The FBI are generally considered to have poor in-house capabilities in developing exploit tool kits or chains for hacking[639] and, though the security services have much greater capabilities, they are reportedly reticent to share them with law enforcement agencies.[640] The FBI therefore use contractors of varying size, though state and local-level law enforcement are believed to rely on buying off-the shelf tools.[641]

The FBI have been known to use zero-day exploits, and likely did in the 2015 child pornography Playpen investigation called Operation Pacifier[642] where, in contrast to the above, access to the vulnerability may have been aided by the NSA.[643] However, due to their cost and the risk of revealing the exploit which would make its future use ineffectual, the FBI use zero-day vulnerabilities relatively sparingly, and there have been few if any substantiated reports of their use by local and state-level law enforcement.[644] Furthermore, an additional consideration for the US Government in using zero-day exploits is the potential for a judge to order that the details of the hacking tools used are released to ensure their validity.[645] For example, one ruling in the case of an individual as part of the Playpen investigation was that the FBI disclose the vulnerability they used to the defence expert.[646] However, the FBI refused to give up their methods for fear of making the exploit ineffectual for future cases, and so the judge dismissed the evidence.[647]

The US Government did actually set up a formal procedure, known as the Vulnerability Equities Process (VEP),[648] that law enforcement agencies should use when finding a vulnerability to determine whether to use it or disclose it to the relevant vendor for patching. This involves reporting the vulnerability to an interagency Equities Review Board (ERB)[649] for a decision, who use a "deliberate process that is biased toward responsibly disclosing [a] vulnerability".[650] A White House Cybersecurity Coordinator outlined the following factors that the ERB consider before making a decision[651]:

- How integral is the vulnerable system to the core internet infrastructure?

---

[636] Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755-56 (S.D. Tex. 2013).

[637] Cardozo, N. 2017. Expert interview conducted for this study.

[638] *Id.*

[639] Bankston, K. & Cardozo, N. 2017. Expert Interviews conducted for this study.

[640] *Id.*

[641] Cardozo, N. 2017. Expert Interviews conducted for this study.

[642] Heath, B. 2016. FBI Ran Website Sharing Thousands of Child Porn Images. USA Today http://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346.

[643] Cox, J. 2016. The Other Reason the FBI Doesn't Want to Reveal Its Hacking Techniques. Motherboard.

[644] Cardozo, N. 2017. Expert interview conducted for this study.

[645] *Id.*

[646] Camarda, B. 2016. Judge tosses evidence in FBI Tor hacking child abuse case. Naked Security by SOPHOS.

[647] *Id.*

[648] Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process. 2010. Found at https://www.eff.org/files/2016/01/18/37-3_vep_2016.pdf.

[649] *Id.,* p. 3.

[650] Daniel, M 2014, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities", White House Blog, ("Daniel Blog Post"), https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

[651] *Id.*

- Does the vulnerability impose significant risk if left unpatched?
- How necessary is the intelligence that could be gained from exploiting the vulnerability and could it be gained by other means?
- Could the vulnerability be utilised for just a short period of time before it is disclosed?
- How likely is it that the vulnerability could be discovered by someone else, how much harm could they do with it, e.g. if it was found by a criminal group, and would any exploitation be likely detectable?
- Can the vulnerability be patched or otherwise mitigated?

Much of the work around the VEP is classified and there have been calls for it to be more formalised with more stringent oversight mechanisms, amongst other suggestions.[652] However, advocates of the VEP have stated that it could present the Federal Government with "a better chance at serving national security, commercial, and personal computing security interests".[653]

Hacking practices by the security services

Whilst the Secret Services have not commented on any official involvement in government hacking, work by researchers and document leaks have provided insight into their activities. The National Security Agency are considered to possess the most advanced capabilities of hacking out of any government agency – much more than at law enforcement level – with robust teams both in-house and under contract developing exploit tool chains.[654] The NSA are responsible for foreign intelligence and counterintelligence through the monitoring of networks and communications data – 'signals intelligence' (SIGINT)[655].

Whilst government legislation does not reference hacking specifically, it is most likely that NSA's use of hacking is regulated through the Foreign Intelligence Surveillance Act (FISA).[656,657] Officials must apply (where possible) for a court order which may be issued on grounds of probable cause using the required minimisation procedures.[658] The process is considered to be analogous to law enforcement applications for a warrant under Rule 41 of the Federal Rules of Criminal Procedure.[659] However, there has been criticism about a reduction in scrutiny in comparison to law enforcement, leading to a greater sense of secrecy[660] and less regulation.[661]

Documents provided by Edward Snowden provide details on the NSA's activities to expand the scope of its hacking powers over recent years.[662] These documents suggest that since 2004, an elite Tailored Access Operations (TAO) Unit has been dedicated to increasing the recruitment of hackers and developing new malware tools, typically delivered through phishing emails or watering hole attacks.[663] These tools include the ability to[664]:

---

652 Schwartz, A. & Knake, R. (2016). Government's Role in Vulnerability Disclosure. The Cyber Security Project

653 *Id.,* p. 18.

654 Bankston, K. & Cardozo, N. (2017) Expert Interviews conducted for this study.

655 Nyst, C. (2017) Expert Interview Conducted for this study.

656 50 U.S. C § 1801.

657 Bankston, K. (2017) Expert Interview Conducted for this study.

658 50 U.S. C § 1801 (h).

659 Bankston, K. & Cardozo, N. (2017) Expert Interviews conducted for this study.

660 *Id.*

661 Cardozo, N. (2017) Expert interview conducted for this study.

662 Gallagher, R. & Greenwald, G. (2014) How the NSA Plans to Infect 'Millions' of Computers with Malware. *The Intercept.*

663 *Id.*

664 *Id.*

- Take over a computer's microphone and record conversations, or a webcam to capture images
- Collect internet browsing history records and login details and passwords
- Monitor keystrokes to determine what was typed into a computer
- Examine data from removable flash drives connected to the computer

Furthermore, whilst previously NSA deployed implants "for a few hundred hard-to-reach targets", a more recent, automated system (TURBINE) "allows the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually",[665] suggesting that the NSA is aiming to expand and automate its hacking powers.

[665] Gallagher, R. & Greenwald, G. (2014) How the NSA Plans to Infect 'Millions' of Computers with Malware. *The Intercept.*

APPENDIX 3: BIBLIOGRAPHY

'Greco' Bill, of 2 December 2015, Modifica all'articolo 266-bis del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche.

A Question of Trust. Report of the Investigatory Powers Review by David Anderson Q.C. Independent Reviewer of Terrorism Legislation June 2015.

Abelson, H. et al. 2015. Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. Computer Science and Artificial Intelligence Laboratory Technical Report

ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media (2016) II. Technological and Policy Concerns (C) Law enforcement agencies will increasingly need zero day exploits

ACLU, Second Comment, supra note 54, p. 18

Adamski, Andrzej. 2008. Opinion on the draft law no. 458 amending the Criminal Code, Biuro Analiz Sejmowych, p. 6.

Adamski, Andrzej. 2015. 'Cybercrime Legislation in Poland', National Report for the International Congress on Comparative Law, p. 10.

Amnesty International. 2016. Poland: Counter-terrorism bill would give security service unchecked power. Public Statement. EUR 37/4263/2016.

Any Computer Accessing Electronic Message(s) Directed to the Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Message(s) Delivered to that Account By the Government, No. 3:07-mj-05114-JPD (W.D. Wash. June 22, 2007).

Australian Security Intelligence Organisation Act 1979, Commonwealth Consolidated Acts.

Barth, B (2016). Executive branch concedes Wassenaar Arrangement must be renegotiated, not revised. SC Media.

Bauer, S. and Bromley, M. 2016. The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World. Non-Proliferation Papers by the EU Non-Proliferation Consortium. No. 48.

Bellovin, S.M., Blaze, M., Clark, S. and Landau, S., 2014. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. Nw. J. Tech. & Intell. Prop.

Berger v. New York, 388 U.S. 41, 86 (1967)

Besluit technische hulpmiddelen strafvordering, available here: http://wetten.overheid.nl/BWBR0020444/2013-03-15.

Bowling, B., & Ross, J. 2006. The Serious and Organised Crime Agency: Should we be afraid? Criminal Law Review, December, 1019-1034.

BVerfG, Judgement of the First Senate of 20 April 2016 – 1 BvR 966/09 – paras. (1-360).

BVerfG, Judgment of the First Senate of 27 February 2008 – 1 BvR 370/07 – paras. (1-333),

Camarda, B. 2016. Judge tosses evidence in FBI Tor hacking child abuse case. Naked Security by SOPHOS.

Cameron, D. 2015. PM: spy agencies need more powers to protect Britain, Jan. [Online]. Available:https://embed.theguardian.com/embed/video/uk-news/video/2015/jan/12/david-cameron-spy-agencies-britain-video.

Centre for Democracy and Technology. 2011. 'Going Dark' Versus a 'Golden Age for Surveillance'.

Citizen Lab. 2014. Mapping Hacking Team's "Untraceable" Spyware. Accessed on 28.02.17 at: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

Code de procédure pénale, Article préliminaire. Unofficial translation by John Rason Spencer QC, Professor of Law at the University of Cambridge, accessed on 03.03.17 at: http://www.legislationline.org/documents/section/criminal-codes/country/30.

COM(2017) 10 final (E-Privacy Directive proposal)

Comey, J. 2014. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? FBI News

Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process (2010). Found at https://www.eff.org/files/2016/01/18/37-3_vep_2016.pdf.

Computer Misuse Act 1990 c. 18 Computer misuse offences.

Constitution of the Italian Republic. Official translation accessed on 28.02.17 at: https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf.

Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union, 12 July 2000.

Council of Europe. 2010. Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Discussion paper.

Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016.

COUNCIL REGULATION (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

Cox, J. 2016. Australian Authorities Hacked Computers in the US. Motherboard

Cox, J. 2016. The Other Reason the FBI Doesn't Want to Reveal Its Hacking Techniques. Motherboard.

Cox, J. 2016. What the UK's Proposed Surveillance Law Means for Police Hacking. Motherboard

Coyne, A. 2016. Govt to spend $230m on cyber security strategy. Itnews.

Crimes Act 1914, Sect 70 – Disclosure of information by Commonwealth officers. Commonwealth Consolidated Acts.

Dambrine, B. 2015. The State of French Surveillance Law. Future of Privacy White Paper. 22 December 2015.

Daniel, M 2014, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities", White House Blog, ("Daniel Blog Post"), https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

Data Retention and Investigatory Powers Act 2014.

David Cameron. 2015. PM: spy agencies need more powers to protect Britain, https://embed.theguardian.com/embed/video/uk-news/video/2015/jan/12/david-cameron-spy-agencies-britain-video.

Decisions of the Federal Court of Justice in Criminal Cases (Entscheidungen des Bundesgerichtshofes in Strafsachen – BGHSt) 51, 211.

Decree-Law No. 7 of 18 February 2015, 'Misure urgenti per il contrasto al terrorismo anche di matrice internazionale'.

Diffie, W. and Hellman, M. 1976. New Directions in Cryptography. IEEE Transactions in On Information Theory. Vol. IT-22, No. 6, November 1976.

Digital Agenda 2014-2017, German Federal Government. Accessed in EN on 24.01.17 at: https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf?__blob=publicationFile&v=6.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. See also the Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.

Directive 2011/36/EU of the European Parliament and of the Council of 5 April 20112 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA.

Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

Docket Folder, Proposed Amendments to the Federal Rules of Criminal Procedure

Draft Investigatory Powers Bill, November 2015.

Duffy, C. & Main, L. 2015. Australian police and Defence Force used infamous Hacking Team, Wikileaks reveals

ECHR cases of Szabo v. Hungary, Zakharov v. Russia.

EDRi. 2016. German surveillance laws: placebos, poison, and also bad sport. Article of 27 July 2016.

Electronic Frontier Foundation. Government Hacking and Subversion of Digital Security. Accessed on 06.03.17 at: https://www.eff.org/issues/government-hacking-digital-security.

ENISA and Europol. 2016. On lawful criminal investigation that respects the 21st Century data protection. Europol and ENISA Joint Statement.

Equipment Interference DRAFT Code of Practice, Autumn 2016.

Ermoshina, K., Musiani, F. and Halpin, H. 2017. End-to-end Encrypted Messaging Protocols: An Overview. Accessed on 01.02.17 at: https://hal.inria.fr/hal-01426845/document.

Eur. Ct. H.R., Kruslin v. France and Huvig v. France (Appl. Nos. 11801/85 and 11105/84), judgements of 24 April 1990, Rep. 1997-II.

European Commission. 2016. Commission proposes to modernise and strengthen controls on exports of dual-use items.

European Parliament resolution of 17 December 2015 on arms export

European Parliament resolution of 21 May 2015 on the impact of developments in European defence markets on security and defence capabilities in Europe

European Parliament resolution of 5 February 2014 on the ratification of the Arms Trade Treaty.

European Parliament resolution of 8 September 2015 on human rights and technology

European Parliament, Council and Commission joint statement on the review of the dual-use export control regime (2014)

European Parliament. 2015. Follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens. P8_TA(2015)0388.

European Union Agency for Fundamental Rights. 2015. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member States' legal frameworks.

FED. R. CRIM.

Filiol, E. 2005. Computer Viruses: from theory to application. Springer.

Franco-German initiative on internal security in Europe, Joint statement by the French and German Ministers of the Interior. 23 August 2016, Paris.

Freedom of Information Act 1982 – Sect 37, Documents affecting enforcement of law and protection of public safety. Commonwealth Consolidated Acts. (2) (b).

French Code de procédure pénale

Gallagher, R. & Greenwald, G. 2014. How the NSA Plans to Infect 'Millions' of Computers with Malware. The Intercept.

Galli, F. 2016. The interception of communication in France and Italy – what relevance for the development of English law? The International Journal of Human Rights. Volume 20(5).

Galvagna, C. 2016. German Foreign Intelligence Bill Fails Human Rights Standards.

Gambini, M. 2014. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: ITALY.

German Basic Law (GG)

German Code of Criminal Procedure (StPO)

Gewijzigd Voorstel van Wet – Computercriminaliteit III, 20 December 2016.

Griffin. A. 2016. WhatsApp privacy under threat as France and Germany push EU to allow states to break encryption. Article for The Independent. Accessed on 02.03.17 at: http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-privacy-under-threat-as-france-and-germany-push-eu-to-allow-states-to-break-encryption-a7204961.html.

Grubbs, 547 U.S. at 96-97

Heath, B. 2016. FBI Ran Website Sharing Thousands of Child Porn Images. USA Today http://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn- images/79108346.

Human Rights Council resolutions 28/16 of 26 March 2015 and 32/13 of 1 July 2016; and A/HRC/27/37.

IACP Summit Report. 2015. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence.

Immenkamp, B (European Parliamentary Research Service). 2017. Review of dual-use export controls: European Parliament Briefing: EU Legislation in Progress. Accessed on 10.03.17 at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf.

Intelligence Services Act 1994. Section 7. Authorisation of acts outside the British Islands.

International Telecommunication Union (2008) Technical Aspects of Lawful Interception. ITU-T Technology Watch Report 6

Interview with David Anderson QC, June 2015. Surveillance powers: New law needed, says terror watchdog.

Investigatory Powers Act 2016.

Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny (2016).

Italian Court of Cassation, Division V, Decision No. 24695, of 14 October 2009.

Italian Court of Cassation, Division VI, Bisignani Case – Decision No. 254865, of 27 November 2012.

Italian Court of Cassation, Division VI, Musumeci Case – Decision No. 27100, of 26 May 2015.

Italian Court of Cassation, Joint Sessions, Scurato Case – Decision No. 1 July 2016.

J.J. Oerlemans, Hacken als opsporingsbevoegdheid, 2011, pp. 901-903. See also B.J. Koops & Y. Buruma (2007), 'Formeel strafrecht en ICT', in: B.J. Koops (red.), Strafrecht en ICT, 2e druk, Den Haag: Sdu 2007, p. 118.

J.J. Oerlemans, Hacking without a legal basis, Leiden Law Blog, 30 October 2016. Available at: http://leidenlawblog.nl/articles/hacking-without-a-legal-basis.

J.J. Oerlemans, Investigating cybercrime, Chapter 8: Performing hacking as an investigative method, January 2017, p. 250.

Järvinen, H. 2016. France and Germany: Fighting terrorism by weakening encryption. Article for EDRi. Accessed on 02.03.17 at: https://edri.org/france-germany-fighting-terrorism-by-weakening-encryption/.

Jennifer Valentino-DeVries and Danny Yadron, FBI Taps Hacker Tactics To Spy on Suspects, WALL STREET JOURNAL (Aug. 3, 2013).

Joffe v. Google, 746 F.3d 920, 926-36 (9th Cir. 2013)

Judgment K 23/11 of the Constitutional Tribunal of 30 July 2014. 80/7/A/2014. Official translation accessed on 10.02.17 at: http://trybunal.gov.pl/en/hearings/judgments/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/.

Kevin Poulsen, Visit the Wrong Website, and the FBI Could End up In Your Computer, WIRED (Aug. 5, 2014), available at https://www.wired.com/2014/08/operation_torpedo.

Kim, S. 2016. Whose World Is This?: US and UK Government Hacking

Knight, B. 2016. Germany to pour cash into mass surveillance. http://dw.com/p/1Jybl.

Koops, B.J. and Goodwin, M.E.A. 2014. Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law, The Hague/Tilburg: WODC/TILT, available at https://ssrn.com/abstract=2698263.

Koops, B.J., C. Conings & F. Verbruggen. 2016. Zoeken in computers naar Nederlands en Belgisch recht. Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?, Oisterwijk: Wolf Legal Publishers, pp. 51-60.

Korff, D., Wagner, B., Powles, J., Avila, R. and Bürmeyer, U. (2017) Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes. Global Report – January 2017. Available at SSRN: https://ssrn.com/abstract=2894490.

Kozlobscki, N. 2000. The Computer Legal Proceeding 54, p. 619.

Law no 2015-912 of 24 July 2015 related to intelligence – Exposé des motifs.

Liberty Group. 2015. Liberty's response to the Home Office consultation on the Equipment Interference Code of Practice

Liberty Group. 2016. Liberty's summary of the Investigatory Powers Bill for Second Reading in the House of Commons. March 2016.

Library of Congress, Global Legal Monitor. 2016. Germany: Powers of Federal Intelligence Service Expanded.

LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale (1). Accessed on 03.03.17 at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231&categorieLien=id.

Lomas, N. 2016. Encryption under fire in Europe as France and Germany call for decrypt law. Article for TechCrunch. Accessed on 02.03.17 at: https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/.

Luis v. Zang, No. 1:11-cv-884, 2013 WL 811816, at *12-25 (S.D. Ohio, Mar. 5, 2013).

Malgorzata Tomkiewicz, 'Podsluchy operacyjne w orzecznictwie sadowym' [Extra-judicial eavesdropping in case law] (2015) Prokuratura i Prawo 4, 153-171.

Marczak, B. et al. 2015. Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. Munk School of Global Affairs.

Marron v. United States, 275 U.S. 192, 196 (1927).

Mayer, J. 2016. Constitutional Malware. Stanford University, School of Engineering, Computer Science, Stanford, CA, United States.

Mayer, J. 2016. III Rules for Malware: (E) Notice. Constitutional Malware. Stanford University, School of Engineering, Computer Science, Stanford, CA, United States.

Memorandum, Department of Justice to Advisory Committee on Criminal Rules 2 (Sept. 18, 2013).

Memorie van Toelichting Wet Computercriminaliteit III, 2015.

Milmo, C. 2014. Edward Snowden revelations: GCHQ 'using online viruses and honey traps to discredit targets'. Article in The Independent. Accessed on 03.03.17 at: http://www.independent.co.uk/news/uk/home-news/edward-snowden-revelations-gchq-using-online-viruses-and-honey-traps-to-discredit-targets-9117683.html.

Ministerie van Veiligheid en Justitie, Briefa an de Voorzitter van de Tweede Kamer « Wetgeving bestrijding cybercrime », 15 October 2012. Available here: https://www.rijksoverheid.nl/documenten/kamerstukken/2012/10/15/wetgeving-bestrijding-cybercrime.

Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). Democratic Safeguards, Secrecy, and counter-law. Computer network operations and 'rule-with-law' in Australia.

Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). Discussion. Computer network operations and 'rule-with-law' in Australia.

Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). Telecommunications (Interception and Access) Act 1979, CNOs, and counter-law. Computer network operations and 'rule-with-law' in Australia.

Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). The ASIO Act, CNOs, and counter-law. Computer network operations and 'rule-with-law' in Australia

Molnar, A. Parsons, C, Zouave, E. (Forthcoming Paper). The Surveillance Devices Act 2004, CNOs, and counter-law. Computer network operations and 'rule-with-law' in Australia.

Moody, G. 2017. Italy Proposes Astonishingly Sensible Rules to Regulate Government Hacking Using Trojans. Accessed on 28.02.17 at: https://www.techdirt.com/articles/20170216/03431236726/italy-proposes-astonishingly-sensible-rules-to-regulate-government-hacking-using-trojans.shtml.

Omnibus Crime Control and Safe Streets Act (1968), P.L. 90-351, 801, 82 Stat. 197, 212 – provides the US government with procedural regulations surrounding the interception of real-time telecommunications.

Open Technology Institute. 2015. Doomed to repeat history? Lessons from the Crypto Wars of the 1990s.

Opinion no2015-078 of 5 March 2015 on intelligence bill (Délibération no2015-078 du 5 mars 2015 portant avis sur un projet de loi relative au renseignement).

Paganini, P. 2016. ZITiS is the new German Government cyber unit formed in the wake of terror attacks. Security Affairs article. http://securityaffairs.co/wordpress/50297/terrorism/zitis-german-cyber-unit.html.

Pietrosanti, F. and Aterno, S. 2017. Italy unveils a legal proposal to regulate government hacking. Accessed on 28.02.17 at: http://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html.

Poland: Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Translation by the Council of Europe, accessed on 10.02.17 at: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)036-e.

Polish Act of 10 June 2016 on anti-terrorist activities and on the amendments to other acts. Unofficial translation accessed on 09.02.17 at: http://www.legislationline.org/topics/country/10/topic/5.

Polish Code of Criminal Procedure, Act of 6 June 1997. Unofficial translation accessed on 10.02.17 at: http://www.legislationline.org/documents/section/criminal-codes/country/10.

Polish Penal Code: Act of 6 June 1997.

Poulsen, supra note 22.

Principles of German Crypto Policy, Federal Cabinet of the German Government. Bonn, June 2 1999.

Privacy International and Open Rights Group's Submission In Response To The Consultation On The Draft Equipment Interference Code Of Practice (2015).

Quinlan, S. & Wilson, A. 2016. Hacking the Mob with Keyloggers. A Brief History of Law Enforcement Hacking in the United States.

Quinlan, S. & Wilson, A. 2016. Hacking the Onion Router. A Brief History of Law Enforcement Hacking in the United States.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Reporters without Borders. 2012. The Enemies of Internet, Special Edition: Surveillance. Accessed on 06.01.17 at: http://surveillance.rsf.org/en/hacking-team/.

Reuters. 2016. France, Germany press for access to encrypted messages after attacks.

Review Grp. on Intelligence and Commc'n Techs., Liberty and Security in a Changing World 187 (2013), p. 220, cited Id.

Right to personality – Enshrined in Basic Law Article 2.1 in conjunction with Article 1.1 GG.

Rules governing the use of government trojan with respect for individual rights: Summary of the proposed amendments to the Italian Code of Criminal Procedure. Published 01.02.17. Accessed on 28.02.17 at: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.

Sakowicz, Andrzej, 'Art. 267' in Michał Królikowski, Robert Zawłocki (eds.), Kodeks karny. Część szczególna. Tom I. Komentarz do artykułów 117–221, C.H. Beck (2013), p. 439.

Schwartz, A. and Knake, R. 2016. Government's Role in Vulnerability Disclosure. The Cyber Security Project.

Sieber, U. and von zur Mühlen. 2016. Access to Telecommunication Data in Criminal Justice: A Comparative Analysis of European Legal Orders. Duncker & Humblot, Berlin, pp. 441-442.

Statement of Charles Farr. 2014. Case No. IPT/13/92/CH.

Statewatch. 2016. German and French Interior ministers demand EU discussion on undermining encryption. Accessed on 02.03.17 at: http://statewatch.org/news/2016/nov/de-fr-comms-letter.html.

Stein/von Buttlar, Völkerrecht, Cologne, 11th ed. 2005, pp. 186–196; Ipsen, Knut, Völkerrecht, Munich, 5th ed. 2004, pp. 310–318.

Surveillance Devices Act 2004.

Sveen, B. & Ockenden, W. 2015. Hacking Team: Australian Government agencies negotiating with notorious surveillance company, leaked emails show. ABC News.

Telecommunications (Interception and Access) Act 1979.

The International Principles on the Application of Human Rights to Communications Surveillance. 2013. Necessary and Proportionate. Accessed on 03.03.17 at: https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf.

The Wassenaar Arrangement – On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, About Us. http://www.wassenaar.org/.

Thompson, R.M. (2016). Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Congressional Research Service

Timberg & Nakashima, supra note 18.

Timm, T. 2014. The government wants tech companies to give them a backdoor to your electronic life. The Guardian. https://www.theguardian.com/commentisfree/2014/oct/17/government-internet-backdoor-surveillance-fbi.

Treaty on the Functioning of the European Union (TFEU).

U.S. CONST. amend. IV.

UN General Assembly resolution 68/167 of 18 December 2013 on the right to privacy in the digital age.

UN General Assembly resolution 69/166 of 18 December 2014 on the right to privacy in the digital age.

UN General Assembly. 1966. International Covenant on Civil and Political Rights, Treaty Series, vol. 999, p.171, Article 17.

UN General Assembly. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40.

UN General Assembly. 2016. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. A/RES/70/125.

UN General Assembly. 2016. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/71/373.

UN General Assembly. 2016. Right to privacy report of the Special Rapporteur on the right to privacy. A/71/368.

UN General Assembly. 2016. The right to privacy in the digital age. A/C.3/71/L.39/Rev.1.

UN High Commissioner for Human Rights. 2014. The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/27/37.

UN Human Rights Council. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40.

UN Human Rights Council. 2015. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/29/32.

UN. 1948. Universal Declaration of Human Rights. Article 12.

United States Code (U.S.C.)

United States v. Cuevas-Sanchez, 821 F.2d 248, 250 (5th Cir. 1987).

United States v. Karo, 468 U.S. 705, 718 (1984)

United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *3 (D. Neb. Aug. 5, 2016).

United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. Digital Evidence and Electronic Signature Law Review, 13(2016).

Vance, C. Y., Molins, F., Leppard, A. and Zaragoza, J. 2015. When Phone Encryption Blocks Justice. The Opinion Pages. The New York Times, August 11, 2015.

Volz, D. 2015. FBI would gain new hacking power if search warrant rules change.

Vragen van de leden Berndsen-Jansen en Verhoeven (beiden D66) aan de Minister van Veiligheid en Justitie over het hacken van servers door de politie terwijl de zogenaamde «hackwet» nog niet door de Kamer is behandeld (ingezonden 26 augustus 2014). Antwoord van Minister Opstelten (Veiligheid en Justitie) (ontvangen 20 oktober 2014). Zie ook Aanhangsel Handelingen, vergaderjaar 2013–2014, nr. 34. Available here: https://zoek.officielebekendmakingen.nl/ah-tk-20142015-286.html.

VSG NRW (Constitution Protection Act – North Rhine-Westphalia).

Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013).

Warrant. 958 F. Supp. 2d at 759.

Wetboek van Strafvordering.

Wetsvoorstel Computercriminaliteit bij Tweede Kamer ingediend, 22 December 2015.

Why is Apple objecting to the government's order? – Apple letter to customers http://www.apple.com/customer-letter/answers/; http://www.digitaltrends.com/mobile/apple-encryption-court-order-news/.

Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

WODC, De Wet bijzondere opsporingsbevoegdheden – eindevaluatie, 2004. P.145. Available here: https://www.wodc.nl/binaries/ob222-volledige-tekst_tcm28-74925.pdf.

WODC, Het gebruik van de telefoon- en internettap in de opsporing, 2012, p.16. Available here: https://www.rijksoverheid.nl/documenten/kamerstukken/2012/05/25/wodc-rapport-het-gebruik-van-de-telefoon-en-internettap-in-de-opsporing.

CAT: QA-04-17-345-EN-C (paper)
CAT: QA-04-17-345-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 978-92-846-0869-0 (paper)
ISBN 978-92-846-0868-3 (pdf)

doi:10.2861/124431 (paper)
doi:10.2861/251421 (pdf)

Publications Office