Framework Proposal to Regulate Lawful Hacking by Police Within Criminal Investigations

by

Ilia Kolochenko

A Dissertation Presented in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy (Ph.D.)

in Computer Science

CAPITOL TECHNOLOGY UNIVERSITY

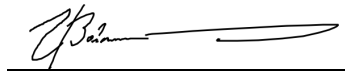
August 2022

Approved:

Dr. Ian R. McAndrew, Chair
Dr. Richard Baker, Associate Dean
Dr. Greg Voykhansky, External Examiner

Accepted and Signed:

Richard E. Baker — October 12, 2022
Richard Baker, PhD, FRAeS — Date


October 12, 2022
Greg Voykhansky, PhD, JD — Date

Ian McAndrew — October 12, 2022
Ian R. McAndrew, PhD, FRAeS — Date
Dean of Doctoral Programs
Capitol Technology University

ABSTRACT

After buying a new automobile, one would unlikely be excited to learn that a local police department has stealthily hacked into the automobile's onboard computer to remotely extract digital evidence of a recent speeding on the highway. The same person would probably also be anxious and uncomfortable upon learning that enacted privacy legislation precludes national law enforcement agencies from using well-known computer hacking techniques to intercept emails and instant messages of organized crime groups implicated in first-degree murders and racketeering, human trafficking, and other nefarious crimes committed in the local area. This qualitative research leverages an exploratory case study design to better understand (i) whether and why police may need to use lawful hacking to collect and seize electronic evidence within criminal investigations of serious and organized crime; (ii) whether and how lawful hacking may be substituted with less intrusive technical or legal means of crime investigation; and (iii) whether and how efficient and cost-effective lawful hacking may be compatible with the rule of law, the integrity of criminal justice system, the individual privacy and other valuable human rights. At the end of this dissertation, the researcher will answer the foregoing questions and produce a jurisdiction-neutral and technology-agnostic framework, composed of 15 mutually supporting sections, offering a multidisciplinary foundation to better regulate lawful hacking within criminal investigations conducted by police and other law enforcement agencies in developed countries.

Keywords: lawful hacking, network investigative techniques, government hacking, lawful interception, law enforcement, digital forensics, criminal justice, cyber law, privacy

DEDICATION

With the utmost gratitude, I dedicate this dissertation to my beloved family for the continuous support, love, and ongoing inspiration I received in abundance during the exciting journey of my doctoral studies, research, and defense, while working full time. Within the foregoing dedication, I wholeheartedly express my most sincere thankfulness to my father who was working around the clock to support me paying for education years ago when I had just started my Bachelor's studies, and to my mother who had sacrificed her own Ph.D. journey to give a birth and to take care of me 35 years ago. God bless them.

ACKNOWLEDGEMENTS

The researcher thanks everyone who was supporting him during the exciting three years of the intensive doctoral studies, research, writing, and preparation for defense. Below is a non-exhaustive list of the outstanding industry practitioners, experts, scholars, and academics whose help, guidance, or advice at different stages of the dissertation writing were immensely valuable for the eventual success of this research:

- Prof. Alexandre Vautravers
- Benjamin Wright, J.D.
- Bertrand Kolb, MAS-CE
- Prof. Burkhard Schafer
- Daniel Drewer, Ph.D.
- George D. Davis III, Ph.D.
- Gordon Platt, Esq.
- Ian R. McAndrew, Ph.D.
- Jan Ellermann, Ph.D.
- Kyung-Shick Choi, Ph.D.
- Nicolas Jondet, LL.M.
- Philipp Amann, Ph.D.
- Samuele De Tomas Colatin, LL.M.
- Stephane Koch, MAS LCE
- Steven W. Wood, D.Sc.
- Prof. Viktor Polic

NB: all individuals from the list above were acting in their personal capacity; no affiliation whatsoever with, or endorsement by, their employers or organizations is implied.

TABLE OF CONTENTS

1. CHAPTER ONE

§ 1.1 Research Background

Decades ago, digital evidence was primarily relevant to investigations of cybercrime or computer-enabled crimes, whilst today even the most trivial domestic or street crimes commonly involve both incriminating and exonerating digital evidence that may be pivotal for the fairness and efficiency of not only a given case, but also the criminal justice system more generally (Kleijssen & Perri, 2017). Modern electronic evidence is widely available in numerous forms and formats, spanning from medical data collected by smartwatches and stored in a cloud to records of blockchain transactions evidencing possible money laundering. Kleijseen and Perri (2017) further crystalize the indispensable role of digital evidence for law enforcement agencies: "nowadays evidence in relation to any crime is increasingly available only in electronic form on computer systems or storage devices and needs to be preserved for criminal proceedings" (p. 149).

The rapid proliferation of digital gadgets, storing gigabytes of digital evidence, may first appear to present a trove of resources to ease the work of police and other law enforcement agencies, helping them to solve all kinds of crimes in a swift and effective manner. In practice, however, the wide availability of affordable electronic devices with a strong encryption enabled by default undermines the investigation and prosecution of organized and serious crime by rendering incriminating digital evidence unidentifiable or unavailable (Europol & Eurojust, 2019). Paradigmatically, the traditional seizure of digital evidence or the lawful interception of electronic communications by police has become futile due to the strong encryption and interrelated security mechanisms, which were originally designed to protect the privacy of legitimate users, but have been misappropriated and misused by serious and organized crime to conceal electronic evidence and to hinder police investigations.

Actually, the “Going Dark” phenomenon, which describes the misuse of encryption technologies by offenders to further their crimes and obstruct investigations, is far from being novel. Back in 2014, Hon. James Comey, then the Director of the FBI, elaborated on the multifaceted challenges of the Going Dark phenomenon during his famous talk at the Brookings Institution (Comey, 2014). His discourse, however, was not groundbreaking per se. Concerns over the increasing misuse of encryption had been voiced three years earlier by Valerie Caproni, then the FBI General Counsel, in her testimony before the House Judiciary Committee (Caproni, 2011). Nowadays, with the abundance of readily available low-cost mobile devices and online services, which are specifically designed to protect user privacy and even provide some level of anonymity, it would be an arduous task to image a single crime—be it an ordinary street crime or a sophisticated computer-enabled cryptocurrency fraud scheme that victimizes millions of naïve investors around the globe—whose investigation would not be impeded by the malicious misuse of strong encryption and interrelated technologies by perfidious criminals.

Resultingly, to tackle the aforementioned challenges, law enforcement agencies need computer hacking to efficiently seize the requisite electronic evidence via lawful hacking, also referred to as “network investigative techniques” (NITs) or “government hacking” by some authors (Liguori, 2020, p. 15). As judicially rationalized by Liguori (2020), the term “lawful hacking” is probably the most suitable one because, on the one hand, a hacking by a government is not necessarily lawful by default, whilst, on the other hand, a government may subcontract lawful hacking to non-governmental entities without violating the law. The efficient and effective operationalization of lawful hacking may be a formidable mechanism to surpass technical barriers to the cost-efficient investigation of serious crimes, as will be demonstrated in this dissertation.

The first cases of lawful hacking can be traced back to 1998, when the FBI installed a back door on a suspect's computer to gather digital evidence, including passwords (Brown, 2020). At the time of writing, the technical nuances, scope and legality of lawful hacking remain largely unsettled around the globe, pouring gasoline on the flame of this vigorously debated and highly controversial topic. Below, this research provides some recent and illustrative examples of the spiraling contentiousness and exacerbating uncertainty of hacking by law enforcement agencies around the world.

In Israel, an explosive journalistic investigation has suggested that Israeli police illegally used advanced spyware, made by the notorious NSO Group, to secretly spy on dozens of domestic journalists, business executives, and politicians; the revelations shook Israeli society and provoked mounting indignation among privacy advocates worldwide (Bergman & Kingsley, 2022). The subsequent internal investigation by the Israeli justice ministry, however, exonerated all the police officers accused of misconduct by confirming that the cyber operations in question had been duly performed after valid court approval and in conformity with the law. In Spain, usage of the infamous NSO spyware "Pegasus" caused significantly more dramatic consequences for the former head of the National Intelligence Centre, who was fired following allegations of unlawful mobile phone hacking and illicit surveillance of Spanish and Catalonian politicians (Wise & Mount, 2022). On the other side of the Atlantic, Canadian Parliament launched an investigation of the allegedly overbroad usage of Pegasus by police in response to heated discussions of possible human rights violations (Forrest, 2022). However, the aforementioned incidents pale in comparison to a newer report accusing police in Pune, India, of hacking into the computers and mobile phones of presumably innocent Indian citizens to plant

fake digital evidence thereon, which would subsequently create a seemingly valid reason for their arrest and prosecution for crimes that were never committed (Greenberg, 2022).

Global legislation on lawful hacking largely varies from one jurisdiction to another. For instance, at the time of writing, Australia is preparing new bills or supplementing the existing laws to further expand police hacking powers both for cyber and traditional crime investigations (Australian Department of Home Affairs, 2021). In contrast, other countries, such as the United States, whilst being known as pioneers of investigatory operations in cyberspace, still have no specific statutory laws to regulate offensive cyber operations by their national law enforcement agencies. The amplifying propagation of advanced technologies in people's everyday lives, ranging from wearable Internet of Things (IoT) devices and Radio-Frequency Identification (RFID) chip implants to elastic cloud computing and 24/7 satellite surveillance, exacerbate the technical complexities of lawful hacking and intricate legal nuances thereof, which should be thoroughly weighed by legislators. Moreover, mushrooming privacy and personal data protection laws appear to be inherently incompatible with the very notion of lawful hacking, creating dormant but highly explosive conflicts on both the national and supranational level with, for instance, the General Data Protection Regulation (GDPR) in the European Union (EU).

§ 1.2 Problem Statement

The deterrence theory, which is discussed below, asserts that systematic or manipulatable impunity spurs and fosters crime growth. Hence, to preserve the sustainable development of society and to safeguard the foundational values of democracy, it is necessary to efficiently deter wrongdoers from breaking the law and committing serious crimes. As elaborated above, lawful hacking has become an indispensable tool in the investigatory arsenal of law enforcement entities to efficiently protect the lives, health, and property of law-abiding citizens from the

nefarious hydra of modern crime. Without lawful hacking, a plethora of dangerous, serious, or hate-driven crimes will remain uncleared and unpunished in perpetuity, leaving millions of aggrieved victims uncompensated and with shattered trust in the capacity of government and law enforcement to protect them. Regrettably, large-scale ransomware attacks, proliferating mobile malware, and disastrous breaches of crypto-stock exchanges have created a subconsciously negative perception of "hacking" in the eyes of laypeople, being conceptually and dogmatically incompatible with justice and the rule of law in people's minds. Furthermore, the insufficient, imprecise, and otherwise flawed regulation of the tactics, techniques, scope, or targets of lawful hacking by police will almost inescapably lead to prosecutorial malpractice, arbitrary application of law, miscarriage of justice, wrongful convictions, and mass violations of individual privacy. Poorly regulated or unregulated lawful hacking also stains the reputation of law enforcement agencies, erodes trust in the government, and chills entrepreneurship in a business climate of uncertainty. Recent scandals implicating "lawful" hacking, which eventually turned out to be unlawful or at least grossly unethical, may create a tectonic shift of public opinion towards a blanket prohibition of all hacking by government for any purposes. Populists and some overly ardent privacy advocates may eventually seize the opportunity to grandstand and, under the guise of privacy protection and other laudable causes, catalyze the annihilation of lawful hacking operations by law enforcement agencies. Resultingly, organized crime and determined recidivists will probably be the only beneficiaries of the simmering hostility towards lawful hacking.

At the time of writing, national legislation of lawful hacking has been predominantly inconsistent and rather resembles an entangled patchwork of isolated rules, volatile case law, and heterogeneous statutory provisions. Even some developed European countries have a polarized approach to the regulation (or non-regulation) of lawful hacking, making cross-jurisdictional

collaboration utterly complex and sluggish. Moreover, given that fragmented electronic evidence may reside simultaneously in multiple countries at once or simply be physically located abroad, pivotal questions of jurisdiction and mutual legal assistance between sovereign states are to be addressed in conformity with foundational principles of international law. It is, therefore, crucial to expeditiously create a foundational and jurisdiction-neutral framework that would design the minimum standards of diligence and care of lawful hacking operations by law enforcement agencies, adequately balancing the oftentimes polarized interests of the government, citizens, victims, and offenders.

§ 1.3 Research Questions

This qualitative research leverages an exploratory case study design—as rationalized in the section below—to answer three subsequent questions formulated in the following order:

RQ1: "What are the key technical obstacles and legal barriers that prevent law enforcement agencies from efficiently investigating serious criminal offenses without lawful hacking?"

RQ2: "How and to what extent can lawful hacking by law enforcement agencies be substituted by less intrusive means of investigations of technical or legal nature?"

RQ3: "How can lawful hacking be regulated by a national legislation to be efficient and to respect privacy and other individual rights, the integrity of criminal justice, and the rule of law?"

§ 1.4 Research Methodology

There are three high-level research methodologies: qualitative, quantitative, and mixed. In any study, an appropriate research design should be thoughtfully selected depending on the research objectives, research questions, existing body of knowledge, available data, and the

accessible means to conduct the research (Creswell, 2014). As elaborated below, after juxtaposing the three competing methodologies, this research applies the qualitative methodology as the optimal one under the integrity of circumstances and in reflection of the researcher's goals discussed in this chapter.

A qualitative methodology, as defined and explained by Creswell (2014), is predominantly used to answer open-ended questions or to explore a novel phenomenon not yet sufficiently studied or understood. The qualitative approach is also gaining and increasing popularity among researchers due to, among other things, "a degree of dissatisfaction with other available research methods" (Salkind, 2012, pp. 13-14). Additionally, Creswell (2014) posits that qualitative research may explore a broad spectrum of multidisciplinary information, spanning from nonparticipant observations and structured interviews to structural analysis of legal documents and governmental publications. Therefore, given the open nature of the research's questions, the comparative novelty of the lawful hacking phenomenon, and the nature of the information and data available to the researcher, this research will rely on the qualitative methodology.

In contrast, a quantitative methodology is mostly used in experiments to test existing theories by exploring the relationships between known variables, which the researcher controls and manipulates during the experiment to answer narrowly focused and specific questions. Within a quantitative study, variables are numeric and can be measured and analyzed by various statistical techniques to reach empirical conclusions (Creswell, 2014). The questions in this research are rather broad and open-ended, whilst the underlying variables are either nonnumeric or simply unknown; therefore, the quantitative method would be inappropriate to conduct and meet the primary objectives of this research.

Additionally, a mixed-methods methodology was also evaluated and considered by the researcher as one of the possible methodologies for this research. As remarked by Creswell (2014), mixed methods may enhance the validity and reliability of a research by combining quantitative and qualitative approaches in one study to cross validate its findings. However, as explained above, it is not possible to apply the quantitative methodology to this research, hence, the mixed methods approach could not be correctly operationalized to meet the research's goals and to answer research's questions. In sum, after thoroughly reviewing the existing research methodologies, a preference was given to the qualitative methodology as the most appropriate one for the nature and environment of this research.

§ 1.5 Research Design and Method

This qualitative research leverages an exploratory case study design, a product of constructivism within the modern philosophy of research (Baxter & Jack, 2008). Whilst a case study design commonly lacks generalizability, it provides a transferability of knowledge and paves the way for the continuation of research, adding maturity to the body of knowledge (Salkind, 2012). Additionally, as pointed out by Yin (2003), when a researcher asks "how" or "why" questions, when a researcher does not control and cannot manipulate the research environment or its variables, or when the research encompasses a novel phenomenon, an exploratory case study is most suitable. Likewise, the case study approach prevails in research when mostly qualitative data is accessible to the researcher (Darke & Shanks, 2002). In continuation, Stępień (2019) suggests that the case study design is effective when dealing with complex and multifaceted questions that have no simple or homogeneous answer. These intrinsic attributes of the case study design are probably among the multiple reasons for its growing adoption by researchers in the fields of law and public policy (Crowe, et al., 2011) and

information systems (Baškarada, 2013), which are addressed in this research in synergy with computer science and criminal justice fields. Therefore, considering the evolution of lawful hacking from its late infancy to an early childhood, the exploratory nature and substance of the research questions, as well as the qualitative data available to the researcher, an exploratory case study design seems to be the most utilitarianly sound and appropriate design for this research. The selected design will likewise help the researcher better grasp the legal subtleties and technical details of the emerging phenomenon of lawful hacking (Hayes et al., 2015). Hence, an exploratory case study design forms the scientific skeleton and framework for this research.

For the research method, document analysis is operationalized as the method to answer the three questions of this exploratory case study research stated above. To increase the reliability and validity of the research method, the researcher will use document analysis to explore documents and archives from multiple trusted sources, including but not limited to scholarly publications on the subject matter, positive and normative legislation, relevant case law and jurisprudence, international treaties that may impact lawful hacking on a national or supranational level, governmental and law enforcement reports, statistics on lawful hacking, as well as contextualized publications and statements by reputable experts and major non-governmental organizations advocating both in favor of and against lawful hacking. For practical reasons and to improve the readability of this dissertation, the document analysis is partially incorporated into Chapter 2 and is then coherently continued in Chapter 3. Other research methods, including but not limited to in-person interviews that could potentially bring additional reliability to the findings of this research, were also thoroughly considered by the researcher and its supervisor but, eventually, were not selected for practical reasons. The applied research method and its rationale are further elaborated and discussed in details in Chapter 3.

§ 1.6 Research Theoretical Framework

This exploratory case study research examines the phenomenon of lawful hacking by law enforcement agencies within criminal investigations through the conceptual prism of the deterrence theory, namely through the general deterrence concept discussed below. First formulated in the 18th century by Cesare Beccaria and then expanded by other legal scholars, the original deterrence theory posits that human beings tend to rationally balance the positive and negative costs of their actions, including the risk of being punished for unlawful activities, consistently preferring actions with the highest gains and lowest costs (Maimon, 2020). In other words, would-be offenders are regarded as pragmatic decisionmakers, who will mindfully avoid a deviant behavior if the negative consequences thereof are sufficiently credible, certain, and painful. Maimon (2020) likewise remarked that, whilst the practical effects of deterrence in cyberspace are currently under-researched, concurrent and mutually supporting scholarly publications and experiments demonstrate that offenders will likely behave differently and refrain from certain illicit actions if they know that they are being monitored and can be unfailingly identified and then, eventually and with reasonable certainty, punished for their wrongs. Deterrence is further typified by general/specific and absolute/restrictive models (Gibbs, 1985). The general deterrence aims to flatly prevent all would-be wrongdoers from engaging in a deviant behavior, whereas the specific deterrence targets recidivism among already-punished individuals. Whilst the aim of the absolute deterrence is a blanket preclusion of criminal behavior by potential offenders, that of the restrictive deterrence is to reduce the severity or frequency of criminally punishable acts.

Despite the ongoing debates and thought-provoking research on the interrelatedness and potentially spurious relationship between punishment and crime rate, it has been generally

accepted that an increase of the "certainty and celerity" of punishment decreases crime rates (Bhattacherjee & Shrivastava, 2018, p. 708). This relationship is an important factor for legislators to consider when enacting or adjusting positive law or discussing normative law (Johnson, 2019). Therefore, the researcher believes that granting police forces a reasonably comprehensive right to conduct lawful hacking operations within criminal investigations to collect otherwise unavailable inculpatory digital evidence will bolster the crime clearance rate and speed, serving as a formidable deterrence both for first-time offenders and seasoned recidivists. Of note, as will be elaborated in the next chapters of this dissertation, the researcher proposes a legalization of lawful hacking operations by police in cyberspace for investigations of only serious and organized crime.

§ 1.7 Research Purpose and Goals

This exploratory case study research aims to comprehensively explore and better understand the compounded array of technical, operational, and legal aspects of lawful hacking to eventually distill its most important elements and then synthesize a multidisciplinary and jurisdiction-neutral framework on sustainable lawful hacking. The framework is designed, among other things, to help lawmakers create or amend a better national legislation on lawful hacking within criminal investigations by police and other competent law enforcement agencies by fairly balancing the reasonable interests of victims, offenders, and any concerned third parties with the efficiency and effectiveness of the criminal justice system. The framework is also intended to improve the existing criminal justice system and to ameliorate legislation on the use of cyber force by law enforcement agencies within criminal investigations, while better protecting privacy and other human rights. In view of the foregoing, this qualitative research can be classified as nonexperimental and applied (Salkind, 2012). The three underlying and

interconnected purposes of the framework, which will be produced at the end of this research, are briefly discussed below.

First, by creating the framework, the researcher purports to provide the legislative and executive (those having a rulemaking authority) branches of government with a concise but comprehensive guide as a basis on which to enact or amend legislation or administrative regulations of lawful hacking in a well-informed, interdisciplinary, and properly balanced manner. Countries with an already-established legislation, which expressly authorizes lawful hacking within criminal investigations, may likewise consider filling the gaps in their statutory law to either provide individuals with a supplementary privacy protection or to enhance the efficiency of lawful hacking operations conducted by national authorities in cyberspace. Additionally, countries without such legislation or with nascent form of the legislation, may leverage the framework as one of the starting points for their legislators.

Second, by creating the framework the researcher intends to equip the judicial branch of government with a simple and understandable list of the most widespread technical concerns, factors, and elements that judges may ponder and asses when, inter alia, allowing or denying motions to conduct cyber operations within criminal investigations as a part of their judicial oversight tasks. The judges may also better comprehend and adjudicate whether police officers surpassed the legally permitted threshold of lawful hacking, or even refer to the framework when assessing the legality or constitutionality of enacted statutory law regulating lawful hacking in jurisdictions where legal systems empower the judicial branch to strike down legislation. Additionally, public prosecutors and practicing criminal defense lawyers may utilize the framework as a general source of multidisciplinary principles of adequacy, proportionality, and appropriateness of lawful hacking methodologies, techniques, and instruments to advance their

pro-conviction or pro-acquittal arguments before a court. Ultimately, both the prosecution and defense will better shape their legal and technical reasoning to avoid wasting judicial resources and to promote the interests of justice.

Third, by creating the framework, the researcher aims to share practical knowledge and technical best practices related to lawful hacking with the law enforcement community, namely with senior staff responsible for drafting internal policies or guidelines designed to elaborate various procedures and precautions required to be completed prior, during, and after lawful hacking operations by police officers. By implementing certain provisions of the framework, law enforcement agencies may reduce undesirable side effects of their cyber investigations, such as exclusion of digital evidence from trial for being procedurally inadmissible or even legal actions against its personnel for abuse of power or infringement of third-party rights. Likewise, the framework will provide a set of internal security and privacy controls aimed to preventing external data breaches, supply chain attacks, and malicious insider activities within law enforcement agencies in charge of lawful hacking operations.

§ 1.8 Research Significance

The cross-disciplinary framework, which this research contemplates creating in Chapter 4, lays the first bricks of the long and sinuous road towards a generally accepted approach to lawful hacking within criminal investigations of serious and organized crime. The approach shall harmonize procedural and substantive criminal law in relation to lawful hacking and various interconnected matters across different jurisdictions. The harmonization would allow law enforcement agencies around the globe to leverage, without fear of breaking the law, the full power of lawful hacking for the benefits of justice and society, while duly protecting individuals' human rights and civil liberties. In continuation, the broader and more efficient investigatory

capacities of law enforcement may likewise deter offenders and reduce crime rate, following the general deterrence theory discussed above. Some foundational and non-contentious elements of lawful hacking may even someday be reflected in a new protocol to the Budapest Convention (discussed in the next chapters) to further promote the consistency and cross-border compatibility of national legislation on lawful hacking, allowing the signatory countries to enhance the interstate collaboration and transborder investigation of serious and organized crime.

§ 1.9 Research Assumptions

For the purpose of this research, it is assumed that various reports, documents, and statistics provided by governmental agencies and other trusted sources contain truthful information that is reasonably accurate and complete. Likewise, it is assumed that public statements by the organizations and experts examined within this research properly and honestly reflect their positions and opinions and do not contain distorted, misleading, or intentionally inaccurate information. It is equally presumed that police officers, public prosecutors, and other members of the criminal justice system act with honesty, integrity, and independence and without bias or impressible self-interest. Their investigatory activities in cyberspace are also assumed to bring sustainable value to society, be compatible with human and civil rights, and duly serve the interests of justice as provided by the law.

§ 1.10 Research Scope, Limitations, and Delimitations

This research primarily covers lawful hacking in developed Western countries by national police forces at both state and federal levels (where such separation of police power exists) and by other national law enforcement agencies tasked with investigating or prosecuting serious crimes. This research focuses on lawful hacking for investigations of serious and organized crime, be it traditional or computer-enabled crime, however, it does not specifically cover

cybercrime that has its own particularities related to investigation. For instance, cybercrime prosecution may necessitate, instead of, or in addition to, identifying and arresting the perpetrators, shutting down an illicit online marketplace or even destroying hacking infrastructure exploited in large-scale phishing or ransomware attacks. Likewise, this research does not address hacking operations conducted by national intelligence or special military units due to the high complexity and obscurity of the applicable legislation, the high level of secrecy surrounding such operations, and the significant implication of politics thereto. Next, this research does not encompass the right to "hack back" in the case of cyberattacks, which is sometimes erroneously referred as "lawful hacking." Equally, this research does not cover the bulk surveillance or interception of electronic communications that are performed by governmental authorities or national intelligence services, outside of the scope of criminal investigations under the provisions of national criminal law.

Moreover, the researcher does not address lawful hacking legislation or case law in developing and underdeveloped countries, being mindful both that their judicial and political systems may first require substantial revision and that lawful hacking is far from being a high priority for their citizens and economies. Importantly, this research does not constitute a comparative study of national law regulating lawful hacking or procedural law governing the admissibility of digital evidence in judicial proceedings. Equally, this research does not attempt to assess or opine on the legality of cross-border lawful hacking under international law. Finally, this research purposely narrows the meaning and scope of "lawful hacking" to (i) intrusive and (ii) remote cyber operations that require compromising or backdooring various digital devices, equipment, or gadgets. Hence, the notion of lawful hacking used in this research excludes the lawful interception of electronic communications by traditional means of interception, the local

exploitation of hardware or software vulnerabilities in mobile devices that are physically accessible to police investigators, and all other comparatively non-intrusive or non-stealth methods of criminal investigations in digital space.

§ 1.11 Definitions of Terminology

This section provides context-specific definitions of key technical and other terms used in this research:

Criminal Offense – a serious criminal act, for example, punishable by at least three years of imprisonment, or otherwise meriting the deployment of lawful hacking due to offense's gravity and the damage it causes to society.

Digital Evidence – any type of digital data, including but not limited to messages, emails, files, logs, raw and binary data, or any excerpts thereof available on any type of digital storage spanning from wearable devices memory to cloud data.

Electronic Evidence – used interchangeably with digital evidence (defined above).

Law Enforcement Agencies – includes national police and all other national law enforcement agencies tasked with investigating criminal offenses or providing technical, scientific, or other types of special support for investigations. This research deploys this term interchangeably with "police" or "law enforcement."

Lawful Hacking – the full spectrum of remote and hacking techniques including but not limited to stealthily penetrating into all kinds of mobile devices, computers, servers, and cloud systems to search for and extract digital evidence to be used in the investigation and prosecution of criminal offenses. The term encompasses installing backdoors on the above-mentioned devices to collect digital evidence in a continuous manner.

§ 1.12 List of Acronyms

ACPO Association of Chief Police Officers

AI Artificial Intelligence

APT Advanced Persistent Threat

BJA Bureau of Justice Assistance (US)

CALEA Communications Assistance for Law Enforcement Act (US)

CCDCOE Cooperative Cyber Defense Center of Excellence (NATO)

CCOA Compliance with Court Orders Act (US)

CCTV Closed-Circuit Television

CDTD Committee on Counter-Terrorism (CoE)

CEPOL European Union Agency for Law Enforcement Training (EU)

CFTT Computer Forensics Tool Testing Program (US)

CI/CD Continuous Integration and Continuous Deployment

CIA Central Intelligence Agency (US)

CIS Center for Internet and Society

CISA Cybersecurity and Infrastructure Security Agency (US)

CLOUD Clarifying Lawful Overseas Use of Data Act (US)

CNI Critical National Infrastructure

CoE Council of Europe

CFAA Computer Fraud and Abuse Act (US)

CPS Crown Prosecution Service (UK)

CSIS Center for Strategic and International Studies

CSLI Cell Site Location Information

CSP Cloud Service Provider

DEA Drug Enforcement Administration (US)

DFIR Incident Response and Digital Forensics

DHS Department of Homeland Security (US)

DNA Deoxyribonucleic Acid

DNS Domain Name System

DoJ Department of Justice (US)

DPO Data Protection Officer

E2EE End-to-End Encryption

EC European Commission (EU)

ECHR European Convention on Human Rights

ECPA Electronic Communications Privacy Act (US)

EDPB European Data Protection Board

EDPS European Data Protection Supervisor

EDRi European Digital Rights

EIO European Investigation Order (EU)

EJN European Judicial Network (EU)

ENISA European Union Agency for Cybersecurity (EU)

EPdO European Production Order (EU)

EPsO European Preservation Order (EU)

FaaS Function-as-a-Service

FDE Full Disk Encryption

FOIA Freedom of Information Act (US)

FoIA Freedom of Information Act (CH)

FOIA Freedom of Information Act (US)

GDPR General Data Protection Regulation (EU)

GPS Global Positioning System

HSM Hardware Security Module

IaaS Infrastructure-as-a-Service

IACP International Association of Chiefs of Police

IoA Internet of Anything

IoT Internet of Things

IPA Investigatory Powers Act (UK)

ISO International Organization for Standardization

ISP Internet Service Provider

JTAG Joint Test Action Group

LEA Law Enforcement Agency

MLAT Mutual Legal Assistance Treaty

NATO North Atlantic Treaty Organization

NCSC National Cyber Security Centre (UK)

NIJ National Institute of Justice (US)

NIST National Institute of Standards and Technology (US)

NIT Network Investigative Techniques

NSA National Security Agency (US)

OFAC Office of Foreign Assets Control (US)

OHCHR Office of the High Commissioner for Human Rights (UN)

OLAF European Anti-Fraud Office (EU)

OSINT Open-Source Intelligence

PaaS Platform-as-a-Service

RAM Random-Access Memory

RFID Radio-Frequency Identification

RIPA Regulation of Investigatory Powers Act (UK)

SaaS Software-as-a-Service

SCRM Supply Chain Risk Management

SoC System-on-a-Chip

S-SDLC Secure Software Development Lifecycle

TOR The Onion Router

UDHR Universal Declaration on Human Rights

UNODC United Nations Office on Drugs and Crime

USB Universal Serial Bus

VEP Vulnerability Equities Process

VoIP Voice over Internet Protocol

VPN Virtual Private Network

WIPO World Intellectual Property Organization

XaaS Everything-as-a-Service

§ 1.13 Dissertation Chapters Summary

Chapter one of this dissertation paints a broad picture of this qualitative research and the underlying reasons that motivated the researcher to study the selected topic and to answer the three research questions. After formulating the research questions, Chapter one briefly explains

and rationalizes the study's methodology, design, and method, both from practical and theoretical viewpoints. Chapter one also sheds light on the scope, limitations, delimitations, assumptions, purpose, and terminology of the research, setting a clearer context for the reader and explaining how the research and its outcomes can be applied in practice to address the problem defined at the beginning of the chapter.

Chapter two of this dissertation explains and defines the scope, purpose, and methodology of the literature review, while further justifying the research method and its suitability for the nature and goals of the research. The reviewed literature covers essential topics for this study, such as (i) the key modern-day challenges that law enforcement agencies face in investigating serious crimes and collecting digital evidence related thereto; (ii) the traditional and emerging procedures for the collection of electronic evidence and their principal deficiencies; (iii) the mandatory backdooring of digital devices to facilitate data recovery and communication interception by law enforcement agencies, as well as other legislative solutions offered to overcome the problems of digital investigations; and (iv) the foreseeable risks and pitfalls of lawful hacking operations. Alternative and less intrusive technical and legal methodologies designed to seize digital evidence within criminal investigations are also discussed at the end of the chapter. Lawful hacking is eventually proposed as a better alternative to other methods of digital investigations targeting organized and serious crime.

Chapter three initially further explains the rationale of the research's qualitative methodology and exploratory case study design, specifically elaborating on the selected design method and its appropriateness for this research. Then, continuing the document analysis commenced in Chapter two for better readability and structural consistency of this dissertation, Chapter three analyzes and concisely compares the broadly varying implementation details, legal

subtleties, and enforcement aspects of existing national legislation on lawful hacking in the selected Western countries. Next, the implications of international law in relation to cyber operations are also briefly discussed. In conclusion, the chapter critically summarizes the findings on existing lawful hacking legislation across different countries, discussing their advantages and disadvantages.

Chapter four, based on the analysis, findings, and discussions in Chapters two and three, meticulously crafts a jurisdiction-neutral and interdisciplinary framework on lawful hacking in pursuit of the underlying purpose of the research. The framework critically examines and systematically assembles such crucial elements of lawful hacking legislation as the question of extraterritoriality, the requirements of proportionality and necessity, the need for judicial supervision, the possibility of independent surveillance, the methods and scope restriction requirements, the reliability of digital evidence preservation and authentication, the issues of transparency and notification to suspects, the unification of hacking methodologies and technical frameworks, and the internal security controls in law enforcement agencies entrusted to conduct lawful hacking within criminal investigations. In essence, Chapter four provides the reader with the interdisciplinary framework on lawful hacking, composed of 15 interconnected and mutually supporting sections, based on the conducted research.

Chapter five of this dissertation concisely answers the three research questions raised in Chapter one. Then, the limitations of the research, related to its scope and to the practical implementation of the framework, are briefly discussed by the researcher. In continuation, the research's contribution to the existing body of knowledge is considered from both practical and theoretical viewpoints, including its examination under the general deterrence theory, justifying the utility and practical novelty of this research. Next, Chapter five suggests possible areas of

future research related to lawful hacking that may deserve further scholarly exploration. Finally, the researcher's recommendations are briefly summarized for the reader in conclusion of the chapter and the dissertation.

§ 1.14 Chapter One Summary

The first chapter of this dissertation has explained and discussed the principal reasons that motivated the researcher to explore the rapidly emerging phenomenon of lawful hacking by law enforcement agencies within criminal investigations of serious and organized crime. Then, after defining three questions that this research aims to answer in the final chapter, a comprehensive discussion of the research methodology, design, and method elaborated their suitability and appropriateness for this specific research and its underlying goals. Next, the research's theoretical and conceptual frameworks were discussed, alongside its underlying purpose and significance. Finally, the scope, limitations, and delimitations of the research, as well as a contextualized definition of terms used in the dissertation, were provided to better set expectations for the reader and to offer a concise guidance for subsequent chapters.

2. CHAPTER TWO

§ 2.1 Literature Review: Purpose

Darke and Shanks (2002) emphasize that a comprehensive literature review and in-depth analysis are central to case study research. According to Creswell (2014), in a qualitative research, literature review plays a pivotal role in elaborating and contextualizing the essence of the research problem to ascertain that the problem has been insufficiently explored in the past and to ensure that both the researcher and the target audience for the research will grasp the underlying issues. Likewise, Creswell points out that literature review helps build solid theoretical and empirical foundations for the research on top of the already existing scholarly and applied knowledge, filling the gaps and adding missing bricks to the body of knowledge to

advance the science. A better understanding of the research's contribution to the current body of knowledge may also be derived from a properly performed literature review, thereby justifying the academic value and practical utility of the research. Importantly, a holistic and thoughtful review of already-published scholarly works gives a due credit to other academics and scholars, who contributed to the body of knowledge and deserve recognition. Finally, the literature review paves the way towards generating ideas of additional research to be conducted in the future (Snyder, 2019).

Following the Creswell's vision, formulated in the previous paragraph, the literature review for this research begins with a multidisciplinary analysis of the contemporary role of electronic evidence in police investigations and the prosecution of serious and organized crime. Then, the analysis comprehensively explores the predominant technical obstacles and legal barriers, along with a convoluted mixture thereof, that prevent or hinder search and seizure of digital evidence by law enforcement agencies. Next, examples of national legislative responses from several jurisdictions to the foregoing problems are critically analyzed through the prism of enacted law and relevant scholarly publications, shedding light on their key strengths and weaknesses. The literature review continues with a review of scholarly publications that advocate for lawful hacking, which favor lawful hacking as an attractive and powerful alternative to the existing and now obsolete methods of electronic evidence search and seizure within criminal investigations by law enforcement agencies. Aiming to maintain impartiality and to inclusively reflect the polarized opinions on lawful hacking, the literature review then also compiles a comprehensive analysis of scholarly publications and expert reports on the risks and threats that may be directly created or tangentially caused by lawful hacking, clearly demonstrating that lawful hacking is not flawless and must be deployed with due care and diligence. At the end of

the chapter, the researcher likewise proposes several less intrusive substitutes to lawful hacking, both of a legal and technical nature, comparing their intrinsic and extrinsic advantages and disadvantages, as well as analyzing whether and to what extent they can replace lawful hacking within contemporary criminal investigations. Upon familiarizing itself with the literature review in this chapter, the reader should have partial answers to the first two questions of this research and be well equipped to move to Chapter 3 of the dissertation, and then to Chapter 4 that eventually designs a jurisdiction-neutral and interdisciplinary framework for lawful hacking based on the performed analysis.

§ 2.2 Literature Review: Methodology and Topics

As elaborated below, this qualitative exploratory case study research incorporates the methodology of the literature review developed by Creswell (2014). At the beginning, keywords—relevant to the research—were identified and then searched within peer-reviewed literature, books, and conference reports through various paid and freely accessible online libraries, archives, and databases by using their built-in search mechanisms and those of Google Scholar. To conduct a comprehensive and inclusive scientific literature review, Creswell (2014) suggested a minimum threshold of 50 scholarly publications to be studied and considered by researcher. This research went through and analyzed over 250 publications about, or related to, the three research questions formulated in the previous chapter. The studied publications covered various interconnected topics from the disciplines of computer science (e.g., digital forensics, encryption and anti-forensics, modern hacking techniques and offensive cyber operations, cybersecurity hardening, and cyber-defense), law and jurisprudence (e.g., national substantive and procedural criminal law, evidence law, constitutional law, lawful interception and telecommunications law, privacy and data protection law, and international public and private

law), and criminal justice (e.g., criminology, digital criminalistics, penology, victimology, deterrence and crime prevention, social and economic impact of crime, and law enforcement operations management).

The selected literature was comprehensively reviewed, read, and cited and then systematically complied in the Bibliography section of this dissertation, pursuant to the 7th edition of APA guidelines (APA, 2020). This literature review relied on general, technology-focused, and legislation-focused online libraries and databases to identify a comprehensive pallet of relevant publications. Below is a non-exhaustive list of the representative scholarly libraries and online resources used by the researcher for literature review:

- ACM Digital Library,
- De Gruyter,
- HeinOnline,
- IEEE Xplore,
- JSTOR,
- ProQuest,
- ResearchGate,
- SAGE Journals,
- ScienceDirect,
- Taylor & Francis Online, and
- Wiley Online Library.

The literature review preferred scholarly works published within the past five years (i.e., 2018–2022). However, to ensure a comprehensive understanding of the historical evolution of the explored phenomenon, each relevant keyword was also searched without filtering for

publication a time. Additionally, being mindful of the pivotal role played by law enforcement and administrative agencies within the context of the research problem, the literature review also encompassed public websites, archives, and social networks of Western law enforcement agencies through manual searches, Google, and special automated tools designed for Open-Source Intelligence (OSINT) research. Most pertinent or otherwise important documents, such as those capable of providing novel or unobvious knowledge to the reader of this dissertation, were incorporated into this research and cited in the Bibliography. Finally, to ensure a two-sided and fairly balanced approach to the research, websites of reputable nongovernmental organizations and subject matter experts, namely the opponents of lawful hacking, were also comprehensively explored during the literature review process. Their works were discussed and juxtaposed with the publications from proponents of lawful hacking, allowing the reader to critically compare the contrasting positions in relation thereto. In the next section, the researcher commences the literature review with a brief discussion of whether, to what extent, and why electronic evidence is required in contemporary criminal investigations of serious and organized crime.

§ 2.3 Role of Digital Evidence in Criminal Investigations

Modern-day criminal investigations incrementally rely on diversified forms of electronic evidence in virtually all type of crimes. The U.S. National Institute of Justice (NIJ) provides a broad definition of digital evidence within the context of criminal investigations (National Institute of Justice, 2022): “information stored or transmitted in binary form that may be relied on in court” (para. 2). This definition covers both common electronic evidence (e.g., emails or SMS messages) and more exotic digital artifacts (e.g., cloud metadata or Global Positioning System [GPS] location history from wearable gadgets). In continuation, the FBI features an article (May, 2021) that says that “digital evidence surfaces in virtually every type of

investigation conducted by local police, […] offering information necessary to support or refute criminal charges, find accomplices, obtain criminal intelligence, and protect the public" (paras. 1-2). Indeed, electronic evidence, interchangeably referred to as "digital evidence" in this research, is located almost everywhere.

Automated video surveillance on highways and onboard electronics embedded into automobiles help police officers to establish the truth in investigations of grave traffic accidents. GPS tracking and cell phone geolocation data, for example, data available via Google's Sensorvault database, is being increasingly utilized by police to identify suspects in serious crimes including kidnapping, armed robberies, and murders (Valentino-DeVries, 2019; Cellbrite, 2019). On the other side, exonerating digital evidence, collected from wearable gadgets such as Fitbit or Apple Watch, is being progressively leveraged by criminal defense attorneys with increasing frequency and success to prove the innocence of their clients and prevent wrongful convictions, stemming from careless police investigations or biased prosecution, sometimes verging on prosecutorial misconduct (Chauriye, 2016). That is to say, digital evidence is not just a sharp sword in the hands of prosecution, but may also be a tenable shield for defense against criminal charges. For defense attorneys, using digital evidence is not an easy task, however, and may require supplementary efforts to prove, for instance, that the defendant was wearing the device in question when the crime was committed.

The Cloud Evidence Group of the Cybercrime Convention Committee (T-CY), which represents the signatory states to the Budapest Convention on Cybercrime that is discussed below, highlighted in their milestone report that:

> Beyond cybercrime per se, evidence in relation to any crime now often stored in electronic form on computer systems and often in foreign, unknown, multiple or shifting

> jurisdictions. Most international requests for data are thus related to fraud and financial crime followed by violent and serious crime ranging from murder, assault, smuggling of persons, trafficking in human beings, sextortion and other sexual crimes, drug trafficking, money laundering, terrorism and the financing of terrorism, extortion and, in particular, child pornography and other forms of sexual exploitation and abuse of children. Predictions are that cybercrime as well as other crime involving electronic evidence will increase significantly with every month. (T-CY Cloud Evidence Group, 2016, p. 6)

Paradigmatically, the number of criminal offenses—both computer-enabled and traditional "street" crimes—whereas the totality of relevant evidence is available only in electronic format is constantly mounting, creating a tectonic shift towards the indispensability of digital evidence for criminal justice (Kleijssen & Perri, 2017). Electronic evidence can be obtained through the process of digital forensics that is briefly explained and discussed below.

§ 2.4 Digital Forensics in Criminal Investigations

Digital forensics can be defined as a "field of forensic science that is concerned with retrieving, storing and analyzing electronic data that can be useful in criminal investigations […] including information from computers, hard drives, mobile phones and other data storage devices" (National Institute of Standards and Technology, 2022, para. 1). Digital forensics typically involves interconnected subprocesses including but not limited to the identification, preservation, acquisition, authentication, inventory, and analysis of electronic evidence, which are completed by preparing a report and, when necessary, providing expert testimony in court to explain the findings and their possible meaning to the court or jury. It is essential to conduct all steps of digital forensics with diligence and care, painstakingly protocoling the work performed

to prevent the loss or unintentional corruption of seized digital data that may jeopardize the integrity of evidence and eventually make it non-adducible in a court of law.

Modern digital forensics relies on a mature and well-established body of knowledge that is corroborated by an abundance of scholarly literature on the subject matter, case law, and a growing set of digital forensic frameworks and standards validated in court proceedings. Back in 2004, the NIJ released a detailed guide to digital evidence collection for U.S. law enforcement agencies, providing case studies from practice, technical examples, and samples of different forms and documents required to accommodate the digital evidence collection process (National Institute of Justice, 2004). Since then, the volume of peer-reviewed scientific publications and official guidelines by authorities on electronic evidence has been growing incrementally around the globe, addressing reasonable concerns over the quality, reliability, and eventual admissibility of digital evidence in court proceedings (Reedy, 2021; Stoykova, 2021). For example, in their recent assessment of the available scientific foundation of contemporary digital forensics, National Institute of Standards and Technology (NIST) experts enumerated the existing international standards (e.g., those published by the International Organization for Standardization [ISO]) related to digital forensics and closely interrelated areas, such as e-discovery (Lyle et al., 2022):

> **ISO/IEC 27037:2012** — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.
>
> **ISO/IEC 27041:2015** — Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method.
>
> **ISO/IEC 27042:2015** — Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence.

> **ISO/IEC 27043:2015** — Information technology — Security techniques — Incident investigation principles and processes.
>
> **ISO/IEC 27050:2018-2021** — Information technology — Security techniques — Electronic discovery. (p. 26).

In the same publication, NIST experts adduced a non-exhaustive list of reputable organizations and institutions that develop and maintain various guidelines and frameworks on digital forensics to be used by law enforcement agencies, prosecutors, and judges (Lyle et al., 2022):

> Scientific Working Group for Digital Evidence (**SWGDE**),
>
> Organization of Scientific Area Committees (**OSAC-DE**),
>
> High Technology Crime Investigation Association (**HTCIA**),
>
> International Association of Computer Investigative Specialists (**IACIS**),
>
> European Network of Forensic Science Institutes (**ENFSI**), and
>
> International Society of Forensic Computer Examiners (**ISFCE**). (p. 25)

In its own contribution to the body of digital forensics within criminal investigations by law enforcement agencies, INTERPOL maintains detailed guidelines for national law enforcement agencies for managing forensic laboratories (INTERPOL, 2019). In addition to the detailed instructions on digital forensics processes and the underlying technical procedures, spanning from electronic evidence acquisition to report writing for judicial proceedings, the INTERPOL guidelines cover best practices on physical security and access management in police laboratories, employee recruitment and screening, hardware and software equipment management, dossier and case administration, and quality assurance procedures. The European Union Agency for Law Enforcement Training (CEPOL) likewise offers a broad spectrum of digital forensics training and courses to promote the efficiency, consistency, and quality of

digital forensics across European law enforcement agencies (CEPOL, 2022). Interestingly, European agencies such as the European Anti-Fraud Office (OLAF) have developed their own guidelines and procedures for digital forensics, designed to improve its efficiency and to better meet their organizational goals (OLAF, 2016). Finally, in the United States, the Computer Forensics Tool Testing Program (CFTT), maintained by the NIST and the Department of Homeland Security (DHS), is designed to validate the reliability of forensic software in a vendor-neutral and comprehensive manner, once again evidencing the high maturity of the modern industry of digital forensics (NIST, 2019). In the next few sections, the researcher will explore and concisely discuss the most common avenues for collecting digital evidence within contemporary criminal investigations.

§ 2.5 Existing Mechanisms for Collecting Digital Evidence

Some scholars indicate that the increasing availability of big data and the impressive progress made in machine learning and Artificial Intelligence (AI) technologies can accelerate and facilitate criminal investigations, while enhancing preventive policing (where the national legislation permits so) and fraud detection (Quattrocolo, 2020). Thus, it may first appear that digital forensics is an omnipotent and armor-piercing weapon in the prosecutorial arsenal of law enforcement agencies, apt to swiftly ferret out virtually any digital evidence to corroborate criminal charges and solve any crime. In reality, however, contemporary digital forensics is a burdensome and thorny practice, riddled with sophisticated pitfalls and disguised traps. Prior to delving into the multidisciplinary realm of the modern digital forensics, populated by technical hurdles and legal challenges, the researcher will first shed some light on principal avenues for collecting digital evidence within modern criminal investigations. Of note, depending on the

jurisdiction, the existing mechanisms of electronic evidence collection, explored below, may vary procedurally and operationally, sometimes in sharp contrast from one country to another.

§ 2.5.1 Seizure of Electronic Devices

Physical seizure of computers, portable electronic devices, or wearable gadgets during a search equipped with a warrant – would, theoretically, be the most straightforward and easy way to obtain digital evidence within a criminal investigation (Jarrett et al., 2009). Back in 2003, comprehensive guidelines on the due process for seizing digital evidence from both individuals and businesses were already available in the United States (Office of Justice Programs [OJP], 2003). The grim reality and the numerous landmines hidden on the thorny road of physical seizure of electronic evidence are concisely examined and discussed in the next paragraphs.

Commonly, national criminal procedure law governs the seizure process and any exceptions thereto (e.g., warrantless searches in case of exigent circumstances or the imminent risk of crucial evidence being destroyed). In turn, this area of law may be influenced and shaped by, inter alia, constitutional law, offering a better protection to suspect (Priester, 2019). Majority of the developed countries have developed internal guidelines and continually revised manuals for law enforcement professionals, aiming to ensure the lawfulness, high quality, and efficiency of police raids involving seizure of digital records, including publications in the United Kingdom (Crown Prosecution Service, 2022) and the United States (National Institute of Justice, 2020) for law enforcement officers. The legality of search and seizure is a key metric of investigation's eventual success, as any electronic evidence collected in violation of a procedural or substantive law will likely be inadmissible in court of law, though the strictness and formalities of exclusionary provisions widely varies from one jurisdiction to another.

Data storage has already experienced a massive shift to a multicloud and hybrid-cloud environment, making its physical location highly volatile or simply unknown. Resultingly, the traditional on-premise search and seizure process for digital evidence is gradually losing its former importance and power within contemporary criminal investigations, subject to some narrow exceptions. Importantly, such exceptions usually relate to petty, juvenile, or otherwise minor criminal offenses: organized crime aptly misuses modern technologies to make physical seizure of electronic devices futile, as will be discussed in greater details in the upcoming sections of this chapter. Nonetheless, if the precise location of a digital evidence is known, if a search and seizure warrant from a judge or other competent magistrate can be obtained, and if no reasons exist to believe that something will hinder the confiscation or subsequent search of digital equipment, then physical search and seizure still remains the easiest and probably the most cost-efficient way to collect inculpatory digital records for investigation (US Secret Service, 2015). As will be demonstrated below, in investigations of organized or serious crime, successful cases of efficient physical search and seizure are virtually non-existent.

§ 2.5.2 Provision of Data by Service Providers

Nowadays, law enforcement agencies may find an immense volume of invaluable data collected and processed by Internet Service Providers (ISPs), operators of mobile messengers, and mushrooming Software-as-a-Service (SaaS) platforms, public Cloud Service Providers (CSPs), and other technology companies that offer, rent, or sell digital services on the Internet. Whilst some of them rarely contain valuable information, such as public twits, others may be decisive for criminal investigations, for example, direct messages between Twitter users or IP address of their last logins. In this research, ISPs, SaaS, and CSP providers are collectively referred to as “service providers,” unless otherwise noted.

Tech giants and transnational service providers, such as Facebook or Google, know virtually everything about a significant number of their unwitting users. The data in their possession may include such sensitive information as a user's current location and travel history, friends and contacts, history of online purchases and payments, food tastes, political and religious views, mental and physical health problems, and even sexual preferences or diseases (Cyphers & Gebhart, 2019). This abundance of data is, however, far from being easily accessible to law enforcement agencies, as will be discussed in detail in the upcoming sections.

Depending on the jurisdiction, various official and informal mechanisms are available to law enforcement agencies to request customer-related information from service providers. The information may be classified into three distinct categories: subscriber information, communications metadata and communications content. The first category represents general information about a user, for example, its name, email, and IP addresses of registration and last logins. Subscriber information is usually considered less sensitive than are the other two categories, and sometimes may even be disclosed upon an informal request from a national or even foreign law enforcement agency. Communications metadata is considered to be more sensitive and private, representing information such as recipients of an email or the timestamp when the email was sent. The third category—communications data—is the most sensitive one and contains such confidential content as the actual text of an email or instant message sent over WhatsApp or Viber. Interestingly, in the European Union—within the context of the European Preservation Order (EPsO) and European Productions Order (EPdO) that were not yet implemented at the time of writing—data classification offers more granularity, with four distinct classes of data: subscriber data, access data, transactional data, and content data (European Commission, 2018).

Varying across different countries, the subtle process of formal information request from a service provider may be differently named and be of an idiosyncratic nature. The most common examples are subpoena, data production request, warrant, and special court order, whereas the name usually reflects the nature and procedural stage of the request, its type, and the sensitivity of the information sought, as well as its legally binding effect and available recourse (if any) to appeal against the order. For example, in some jurisdictions, if an informal request by police is ignored by a service provider, then a warrant signed by a public prosecutor is usually issued. If the warrant is also ignored or contested by the service provider on technical or legal grounds, then a binding court order—usually backed with harsh penalties for noncompliance—may be issued to finally summon the data. Sometimes, depending on the context and place of the investigation, a data production court order can be appealed by the service provider in higher court. In other countries, the process is more straightforward and offers no opportunity to contest it unless specifically provided by law.

In most countries, a court order is predominantly required to disclose communications data, logically offering the strongest protection for the most sensitive information. Some states may incorporate the rules on data production directly into their criminal procedure law, while others possess separate or supplementary laws, regulating access to data stored by third parties and governing certain procedural details. For example, in California, a state law obliges electronic communication service providers to inform the Office of the Attorney General about, and it keep informed about any updates, how and who law enforcement officers shall contact to serve subpoenas, court orders, or search warrants to obtain electronic records within criminal investigations (California Office of the Attorney General, 2022).

Usually, digital data production requests must selectively ask for specific information that is directly relevant to the criminal investigation in question, wherein the nature and volume of the requested data shall likewise be proportional to the gravity of the offense (UNODC, 2019). At the time of writing, the most recent transparency report by Microsoft tellingly illustrates the situation: for the second half of 2021, Microsoft received 25,182 requests to disclose data from authorities around the globe, of which 25.18% were rejected. Only 51.59% of the requests seeking communications metadata and 4.26% of the requests seeking communications data were approved by Microsoft, whilst the remaining 18.97% of the requests sought unavailable or non-existent data and, thus, could not be complied with (Microsoft, 2021). Tellingly, the global statistics from Microsoft vary considerably across countries. For instance, in Canada 41.74% of requests were rejected by Microsoft, as compared to 13.13% in the United States, whereas in Switzerland no single request demanding the production of communications data was approved in 2021. Therefore, the collaboration of service providers with law enforcement agencies remains a highly unpredictable and grossly politicized question, as will be elaborated in further details below.

Procedurally, the binding effect of a data request from a law enforcement agency is also quite polarized from one country to another, and depends entirely on the context of the request. A considerable number of tech platforms voluntarily cooperate with national and even foreign law enforcement agencies, having transparent policies on the subject matter and even a dedicated point of contact to rapidly respond to governmental inquiries (National Consortium for Justice Information and Statistics, 2022; Twitter, 2022). However, the rising trends of privacy-by-design and privacy-by-default push service providers to implement a robust privacy protection program, making access even to basic subscriber information more formal and, thus, more burdensome for

law enforcement agencies, for instance, by requiring a warrant for most data requests (Kerr, 2018). Additionally, in the wake of a recent incident in which cybercriminals exploited compromised email systems of law enforcement agencies to serve Apple and Facebook with Emergency Data Requests (EDR) to gain sensitive data of their users (Krebs, 2022), more precautions in relation to data disclosure via the EDR and other mechanisms will likely be implemented by service providers, eventually slowing down public–private collaboration.

§ 2.5.3 Lawful Interception of Communications

Most of the developed states have specific statutory laws to regulate the lawful interception of electronic communications, ranging from now-outmoded conversations over landline phones to digital packets carrying out bytes of human conversations via omnipresent Voice over Internet Protocol (VoIP) technology, allowing national law enforcement agencies to monitor the live communications of suspects (Institute for Human Rights and Business, 2016). Whilst the lawful interception of landline phone communications within criminal investigations have been in place since decades (Kolb, 2007), the interception of VoIP communication remains, at the time of this writing, utterly problematic in many countries. Unsurprisingly, the basic principles of privacy protection implemented by service providers in relation to data production requests also apply to the lawful interception of communications by police within criminal investigations. For instance, in the United States, the Electronic Communications Privacy Act (ECPA) of 1986—one of the federal laws regulating, inter alia, the lawful interception of communications—clearly differentiates between the interception of live communications data, such as oral discussions, and the accompanying metadata, such as dialed phone numbers, unsurprisingly granting a higher degree of protection to the former (Bureau of Justice Assistance, 2022).

Akin to the seizure and subpoenaing of digital evidence, lawful interception mechanisms vary broadly from one jurisdiction to another. They may have such particularities as mandatory preapproval by a special court or a post-hoc ratification in case of emergency, mandatory implementation of turnkey interception technologies by national telecom operators, public disclosure of interception statistics and the number of court-approved requests, or even a notification to the subject whose communications were monitored once the preliminary investigation phase is over, unless an exception applies (European Telecommunications Standards Institute, 2021). The heterogeneity and complexity of the rapidly evolving laws on interception, complemented by administrative regulations or annexes issued by special administrative agencies that may supplement the statutory law in those jurisdictions where so is permitted, make compliance an arduous task for global telecom operators running business across different countries (Vodafone, 2021). Remarkably, in response to the surging volume of VoIP communications and the intensification of video calls, some researchers propose using machine learning technology to swiftly and automatically classify, inspect and analyze lawfully intercepted traffic, providing law enforcement agencies with a readily usable intelligence (Monshizadeh et al., 2018).

Summarizing this section, lawful interception may first appear deceptively unproblematic and simple, but in practice, access to live communications is an excessively complicated and taxing process, both technically and legally. In the next sections of this dissertation, the researcher will review the broad spectrum of primary obstacles that hinder, slow down or even completely thwart traditional digital evidence collection methods. This will help the reader to better understand why lawful hacking becomes an irreplaceable mechanism in modern investigations of organized and serious crime.

§ 2.6 Existing Challenges to Digital Evidence Collection

Relentless technical progress enables anyone to buy a secure mobile device with strong encryption enabled at all layers. For example, a modern iPhone fortifies access to all data stored on the device with unbreakable encryption that any user can enable in one click, alongside the additional security and privacy-enhancing mechanisms (Apple, 2022). Eventually, the fashionable and user-friendly smartphone becomes a virtually unassailable cyber-Fort Knox for law enforcement agents seeking to extract digital evidence from it (Bullock et al., 2020). Users can purchase a smartphone online in a matter of minutes and receive their purchase on their doorstep within an hour. Despite the undisputable benefits and novel opportunities made available by the technical progress for the well-being of society, those benefits are increasingly misused by serious and organized crime to prevent investigations by law enforcement agencies. Those and other problems of a technical, operational, and legal character are discussed in the next subsections of this chapter.

§ 2.6.1 Digital Evidence Volatility

In contrast to data stored on a hard drive or Universal Serial Bus (USB) key, the data present in the Random Access Memory (RAM) of a computer or laptop is highly volatile: a simple reboot will flush its entire content. For practical and privacy-protection reasons, many software applications, such as instant messengers, are increasingly handling and processing a considerable amount of user-generated data, metadata, and forensic artifacts only in RAM, storing no data on the hard drive (Fernández-Álvarez & Rodríguez, 2022). Some data that may be required for a subsequent reuse, such as user's contacts or communications history, may be encrypted and securely stored in a remote cloud database, basically making any search for digital evidence on a seized device futile, unless credentials to log in to the remote service are available

or can be recovered. For these reasons, post-seizure investigation techniques gradually lose their value, as the requisite data is simply unavailable on the seized equipment. Various post-reboot RAM data recovery techniques exist, such as cold-boot attacks, but their applicability is quite narrow and requires certain conditions to be met, namely unimpeded physical access to the investigated machine while it is switched on and the data is still in RAM (Lindenlauf et al., 2015). Likewise, those techniques are usually inefficient against the regular usage of bootable live CDs or USB keys that are purposely designed to emulate the entire operating system in a read-only mode, eliminating any extractable traces from the device after a reboot or shutdown (Majed et al., 2020).

Evidencing the value and importance of data processed in RAM, Hausknecht et al. (2015) suggested that, in some cases, the data extracted from RAM can provide a complete and holistic evidentiary basis that would suffice to bring criminal charges and possibly secure a guilty verdict. Moreover, the study by Hausknecht et al. contends that a significant number of pivotal forensic artifacts, including but not limited to a list of web pages accessed, images or videos viewed, network traffic flow and history of network connections, temporary content and metadata of edited or accessed files, and even fragments of Skype discussions are solely available in RAM, making a post-mortem examination of the hard drive futile. Oftentimes, perpetrators simply do not leave a sufficient digital footprint within a non-volatile storage, or painstakingly clean it up with readily available free or commercial software tools specifically designed to wipe out browsing history, system logs, temporary files, and other electronic evidence (Ölvecký & Gabriska, 2018). Another empirical study performed a series of experiments evidencing that, as compared to conventional hard drive analysis, RAM forensics is among the most efficient methods to extract important forensic artifacts from desktop instant

messengers—namely Skype—including but not limited to the call history, the virtual identities of interlocutors, and even the content of transferred files (Ghafarian & Wood, 2019). One more experimental study demonstrated that RAM analysis can reliably prove whether and when specific Microsoft Office files were opened or edited without relying on modifiable metadata stored on the disk (Al-Sharif et al., 2018). Sadly, these RAM-investigation techniques are almost never applicable in classic law enforcement raids wherein a suspect's device is shut down and physically seized for further investigation and analysis in laboratory.

Moreover, with the rapidly growing number of SaaS services, more and more digital evidence is stored remotely by design and by default, oftentimes being located in foreign countries or even fragmented across several continents. For instance, once a suspect's machine is rebooted, a web-based email system will unlikely leave any content on the hard disk that would be helpful for investigation. Whilst Hausknecht et al. (2015) refer to various forensically sound hardware and software methods to capture and inspect data in RAM, those methods require timely access to unlocked and switched-on machines with ephemeral RAM evidence still residing in the volatile memory. Moreover, during police raids, experienced offenders usually have a "red button" to swiftly flush dynamic data and shutdown all their password-protected and encrypted devices, making their digital equipment uninvestigable (Cummins Flory, 2016). Finally, even when a suspect's live system is readily available without hindrance, due to the lack of forensic personnel and other operational constraints, the investigation can usually be commenced only a few hours, days, or even weeks after the seizure, when the volatile RAM data will be inevitably lost. In sum, whilst being pivotal for many criminal investigations, volatile data stored in RAM can rarely be seized by traditional investigatory methods to be later adduced in court.

§ 2.6.2 Self-Destructing Messages and Steganography

Amid the widespread increase of consumers' reasonable expectations of privacy-by-design and privacy-by-default for electronic devices and online services, most popular instant messengers, including but not limited to WhatsApp, Snapchat, and Instagram, have implemented self-destructing messages that may disappear after a specific period of time or immediately after being viewed by the recipient (Nield, 2022). Taking the red-hot privacy-protection contest one step further, Google implemented a so-called "Confidential Mode" for its flagship Gmail email service, expanding the information auto-destruction regime to emails by hosting their content on Google-controlled servers (Haselton, 2018). Unsurprisingly, the foregoing functionalities have been enthusiastically adopted by seasoned offenders to conceal traces of their misdeeds.

Although it may be technically unfeasible for service providers to instantly delete messages and other data in a definitive manner from their own and multilayered intermediary systems, as well as from backups, the self-destructing messages erect formidable barriers for forensics experts by making indispensable electronic evidence unavailable or unrecoverable. In the past, several reports were published exploring exploitation of critical bugs and vulnerabilities in different instant messengers rendering their self-destruction functionality useless (Jayapaul, 2021), however, the issues were rapidly fixed by vendors, patching the loophole for law enforcement investigations. Moreover, even if some undeleted excerpts of messages remain in some service provider's systems, their extraction—in a forensically sound manner—will be a cost-prohibitive exercise requiring an exorbitant and fantastically unselfish collaboration from the service provider.

Compared to encryption, which is discussed in the next section, steganography represents just a small fraction of the issues faced by digital investigators. Defined by Stanger (2020),

steganography is “the practice of hiding a secret message inside of (or even on top of) something that is not secret, [… for example] embedding a secret piece of text inside of a picture […] or inside of a Word or Excel document” (para. 2). Whilst steganography has been used for centuries, digital steganography is a relatively new derivative thereof, designed to unsuspiciously hide illicit content or secret data inside unremarkable and ordinary files (e.g., images or videos) that will not raise suspicion when opened with a default application (Dickson, 2021). Because of its comparative rarity and the lack of investigative experience related thereto, steganography can be even more problematic for digital investigations than encryption or other anti-forensics mechanisms are. Moreover, experienced offenders may purposely leave their computers unprotected within the reach of police officers, injecting illicit content into legitimately looking data in a stealthy manner, so later the data will unlikely be detected by common forensic toolkits (Wilson et al., 2021). Consequently, after the search and seizure, chances are high that forensic experts will not spot any reportable issues, producing a blank report confirming that no incriminating evidence is found. The erroneous conclusion will confuse and mislead the prosecution, who may eventually believe that the suspect is truly innocent. Importantly, due to a lack of training dedicated to the detection of steganography, the latter can aptly curtail valuable incriminating evidence from the eyes of even most experienced forensics investigators (Mambodza & NagoorMeeran, 2015). In sum, self-destructing messages and steganography become dangerous instruments in the hands of criminals, making traditional searches and seizures fruitless or excessively onerous: the former simply wipes out any extractable data, whilst the latter preserves evidence on the device but makes it invisible to police radars. Both annihilate investigations of serious and organized crime.

§ 2.6.3 Encryption and the "Going Dark" Phenomenon

Encryption has become an inalienable part of the modern cybersecurity, privacy, and compliance. It would be a challenge to find a single company that does not utilize encryption on most of its on-premise or cloud systems, widely available by default by most vendors and manufacturers, to protect its data at rest and in transit from hacking attacks or malicious insiders. Moreover, most countries have a plethora of existing technology laws that regulate encryption in a prescriptive manner, for instance, by imposing mandatory encryption requirements for personal, financial, or healthcare data. Dogmatically, only a small fraction of the existing encryption laws actually covers decryption and the related duties of service providers or their users (Dizon & Upson, 2021). This regulatory imbalance is dual and oxymoronic: on the one hand, it gave birth to the "Going Dark" anti-encryption phenomenon discussed below, on the other hand, it bolstered the rapid development and Internet-wide proliferation of strong encryption.

One of the first public mentions of the "Going Dark" term by a governmental official is attributable to Hon. Valerie Caproni, then the FBI General Counsel, back in 2011 (Caproni, 2011). She described the weakening technical capabilities of law enforcement agencies to intercept and seize electronic communications and digital evidence due to the rising popularization of encryption and non-interceptable channels of digital communications, which could cunningly pass under the outdated radars of law enforcement. Three years later, in 2014, the term was somewhat formally coined by Hon. James Comey, then the FBI Director, during his landmark talk at the Brookings Institution in Washington, D.C. During his historical speech, which promulgated the "Going Dark" term in the media and boosted public awareness about the underlying problem, Comey eloquently described the challenges of soaring encryption misuse by

sophisticated criminals and organized crime, aiming to avoid detection and to escape prosecution:

> Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so. (Comey, 2014, para. 10)

In continuation, Comey (2014) forewarned that technical progress and the concomitant proliferation of portable and mobile devices made the lawful interception of communications technically complex, time-consuming, and onerous for law enforcement. To illustrate this point, he noted that a single suspect could have dozens of unknown, unidentified, and unidentifiable electronic devices—all used to plan and further their crimes, to purchase prohibited goods or weapons, or to communicate with accomplices or even victims—eventually leaving blinded federal agents in an investigatory maze. Even with the authority to search and seize electronic devices, law enforcement simply could not efficiently perform any of those actions, thereby facing condensing investigatory darkness and disorientation. Moreover, the nationwide implementation of then-novel VoIP communication services (e.g., Skype), with their built-in encryption mechanisms or new techniques to encode traffic data, made the lawful interception of electronic communications tremendously resource intensive. Worst of all, court orders demanding that tech companies assist the FBI or other agencies with lawful interception could not be complied with, as even vendors of emerging technologies had no available means or instruments to intercept the electronic communications of their users. The judicial branch eventually faced the convoluted dilemma of determining whether such involuntary disobedience, caused by technical unfeasibility, should be punishable or not.

In relation to stored electronic data, Comey (2014) warned that the problem of encryption was even broader and deeper. The abundance of open-sourced and commercial tools designed to encrypt entire hard drives, disk partitions, or just select files factually annulled the power of a search warrant. The consequence for the investigators was that a computer with a Full Disk Encryption (FDE) became as valuable as a brick. Comey likewise attempted to dispel the popular myth that the FBI could allegedly break into any device and bypass all forms of encryption: he expressly stated that the federal agency had no such means to do so and had never enjoyed having them in the past. Validating the Comey's concerns, a report from the International Association of Chiefs of Police (IACP) stated that:

> [E]ncryption is preventing law enforcement and justice agencies from executing lawful court orders to investigate criminal or terrorist incidents or to secure electronic evidence. Clear and sometimes insurmountable barriers to the access of electronic evidence have been placed in the way of law enforcement seeking to identify suspects and protect communities from further crime. (IACP, 2015, p.3)

On the other side of Atlantic, the spiraling concerns over malicious usage of encryption, eloquently voiced by Comey (2014), were cogently echoed by Europol two years later. Europol unambiguously labeled the malignant usage of encryption by dangerous criminals and terrorists a threat to public order and safety, the efficiency of the criminal justice system, and the rule of law (Europol, 2016). Later on, a joint report by Europol and Eurojust reiterated those increasing concerns, in relation both to stored data and to data in transit (Europol & Eurojust, 2019). Among other things, the report emphasized that a steadily growing number of serious crimes became technically uninvestigable and even undetectable because of the ubiquitous and unbreakably strong encryption. Among the alarming trends, the report highlighted an unprecedented

abundance of low-cost devices and ready-to-use online services on the market, with strong encryption enabled by default, eventually permitting organized crime and transnational criminal syndicates to effortlessly avoid police radars and enjoy impunity.

While the European Union Agency for Cybersecurity (ENISA) later pointed out that no encryption is a silver bullet or panacea (ENISA, 2019), the most recent (at the time of writing) joint report by Europol and Eurojust clarified that:

> The wider usage of encryption technology continues to be increasingly exploited by criminals, both as part of their modus operandi and as a mean to enable secret communication and illegal activities by putting them out of law enforcement's reach. This continues to create challenges for both the law enforcement and the judiciary communities and significantly hampers these authorities' ability to investigate and prosecute. (Europol & Eurojust, 2021, p. 8)

Some legal scholars have also noticed that the increasing number of instant messengers has implemented end-to-end encryption (E2EE) protocols into their desktop and mobile applications by default, under the guise of enhanced privacy protection, making electronic communications undecipherable even if the service provider wished to gain access to them (Pisaric, 2022). Despite that E2EE technology has been available for over a decade, its default usage for instant text messages and voice and video calls is a comparatively novel phenomenon poised to further obstruct, complexify, and slow down criminal investigations, making the "Going Dark" phenomenon even darker.

From a different perspective, it has been asserted that law enforcement agencies equipped with search warrants could swiftly obtain valuable metadata or, under a narrow set of circumstances, even the data itself from cloud backups of Apple and some popular instant

messenger vendors (Pfefferkorn, 2021). Nonetheless, most criminal gangs implicated in a serious, large-scale, or transnational crime, are well aware of such shrinking loopholes and will unlikely ever entrust their backups to a vendor-managed cloud storage. Similarly, whilst both informal and warrant-backed requests for subscriber information by law enforcement may be a powerful investigatory instrument when dealing with first-time offenders, seasoned bandits have countless ways to anonymously acquire disposable SIM cards and register online service accounts with fake or stolen data. Tellingly, the trend of one-off SIM cards was observed back in 2006, when some European countries started to implement a mandatory identity verification procedure requisite to buy a SIM card (Kolb, 2007). Therefore, the foregoing investigatory techniques have narrow and continually diminishing applicability to combat against organized or serious crime. In parallel, more vendors and service providers exacerbate the problem by enabling backup encryption by default, whilst possessing no access to decryption keys.

In its recent report, the Interpol Innovation Center highlighted that encryption is extensively misused by organized crime to incapacitate the investigations of particularly dangerous crimes, including but not limited to human trafficking, racketeering, murders, and the sexual exploitation of children (INTERPOL, 2021). In a joint article, Hon. Catherine De Bolle, the Executive Director of Europol, and Cyrus R. Vance, Jr., the District Attorney of New York County (NY), also expressed their grave concerns over the skyrocketing misuse of unbreakable and available-by-design encryption in modern mobile devices (De Bolle & Vance, 2021). Of note, whilst advocating for the legitimate use of strong encryption to protect privacy, they expressly indicated that all possible areas of criminality, spanning from midsized ransomware gangs to “multi-billion-dollar criminal enterprises” operating in the offline world, were arming themselves with strong encryption to avoid detection and prosecution. They pointed out that the

"Going Dark" phenomenon is not just a European or American problem, but a global challenge particularly troublesome for developing countries lacking the necessary human, technical, and financial resources to conduct digital forensics and investigations.

De Bolle and Vance (2021) further suggested interagency cross-border operations by law enforcement agencies as a possible response to the spiraling proliferation of encryption misuse. To illustrate the point, they mentioned the unprecedentedly successful "OTF Greenlight/Trojan Shield" joint taskforce campaign, which covertly created and operated a company named "ANOM." On the Dark Web, "ANOM" was selling anonymous and encrypted smartphones, advertised specifically as crypto-devices aimed to avoid detection by police and other law enforcement agencies. In reality, however, the cryptophones contained a backdoor functionality, providing the joint task force with an access to all "encrypted" communications. Ultimately, the "ANOM" campaign led to over 800 arrests connected to smuggling, drug trafficking, and aggravated money laundering (Europol, 2021a). Nevertheless, experts reveal that such operations may strongly incentivize organized crime to build and operationalize their own IT infrastructure, invisible and unreachable to law enforcement agencies, which would make cyber investigations even more challenging over time (Napoleon et al., 2021).

Not everyone, however, shares the bedrock concerns of the "Going Dark" phenomena voiced by law enforcement agencies. For instance, over 10 years ago, Swire and Ahmad (2011) argued that the unstoppable penetration of modern technologies into daily life had created a "golden age for surveillance" for law enforcement (p. 1). They pointed out that the unprecedented abundance of metadata, such as location information collectable from cell phones, could generously compensate the loss of access to communications content. Whilst this

statement was technically correct in 2011, the situation is quite different in 2022, as will be elaborated in the next sections of this chapter.

Summarizing this section, the researcher acknowledges that narrowly applicable and typically resource-consuming methods and techniques do exist to bypass, circumvent, or break the encryption of stored data or encrypted communications. Likewise, the researcher is mindful that encryption is a dual-use technology that offers tremendous benefits to society, which may largely outweigh its misuse by organized and serious crime. Nevertheless, in the contemporary climate of privacy-by-design and privacy-by-default, wherein all major vendors vigorously advertise and promote a turnkey E2E encryption amid the growing valorization of privacy protection by consumers, a predominant number of criminal investigations will likely be paralyzed by the misuse of strong encryption in the near future. Whilst discussions about the possible threats of emergent quantum computing are relevant to the existing encryption landscape (Cybersecurity and Infrastructure Security Agency, 2022), at the time of writing, they are rather hypothetical and cannot efficiently help law enforcement to overcome the encryption challenge. In conclusion, from a technical viewpoint, strong encryption may be deservingly named the most frequent and serious technical obstacle that hinders investigations of serious and organized crime.

§ 2.6.4 Anti-Forensics Tools and Techniques

In addition to encryption, skilled and cyber-savvy criminals may also deploy various anti-forensics tools and traps designed to mislead or confuse investigators (Wilson et al., 2021). There are various interconnected approaches to hinder or delay the work of forensic analysts. For example, wrongdoers may use steganography—discussed in a previous section—and similar techniques to hide data in unusual places such as the unallocated space of a hard drive, crypto

containers disguised as legitimate media files, or system registries in Microsoft Windows systems. Whilst those methodologies remain cat-and-mouse games, data wiping is a considerably more perilous anti-forensics tactic for cyber investigators, as a plethora of special tools are readily available for free download or purchase, providing a broad spectrum of advanced features that range from the secure destruction of all data on a disk to the smart and selective cleaning of forensic artifacts (Wani et al., 2020). When artifact-destruction techniques are thoughtfully used by an experienced perpetrator, the chances of recovering any valuable evidence from the device border on zero. Moreover, advanced wiping tools not only clean up all incriminating logs, artifacts, and traces, but do so inconspicuously and almost undetectably (e.g., without leaving any inexplicable "holes" or discrepancies in logs that may indicate the usage of an anti-forensic cleaner). Instead, the tools meticulously replace "bad" events with innocent and banal ones, creating a legitimate picture of perfectly blameless and innocent computer usage (Mistry et al., 2020). Consequently, when a suspect's device is seized, but no incriminating digital evidence whatsoever is eventually found on it, the prosecution's chances of securing a guilty verdict are diminished, compared to a situation in which all suspect's devices are locked and encrypted and the suspect vehemently refuses collaboration with justice. Moreover, after getting a blank report from a forensics laboratory, the prosecutor may start to doubt the eventual culpability of the suspect and may even drop charges. Accordingly, advanced data-wiping tools in the wrong hands can fatally frustrate even a well-prepared investigation and corresponding prosecution efforts to solve a crime.

The more advanced anti-forensics techniques include exploitation of bugs and vulnerabilities in popular forensics toolkits, for example, by freezing the forensics software or corrupting its reports, eventually casting a shadow on its reliability (Mistry et al., 2020; Wilson et

al., 2021). Eventually, particularly inventive offenders may even try to accuse investigators of forging or falsifying electronic evidence, although this vexatious tactic has been shown by the experimental research to be easily rebuttable (Freiling & Hösch, 2018). Sophisticated anti-forensics tools may also convert a seized machine into a technically uninvestigable object by purposely creating millions of fake artifacts instead of, or in addition to, erasing the genuine ones. An advanced anti-forensics tool may, for instance, generate countless files or Microsoft Windows Registry entries with suspicious patterns and attributes or containing some well-known illicit content, spanning from child pornography to bitcoin addresses implicated in sextortion or ransomware. Eventually, police investigators are overwhelmed with an unworkable number of inseparable digital records, wherein distinguishing the suspect-created traces from randomly generated ones is arduous or even technically impossible (Wilson et al., 2021). Considering the growing convergence of organized crime and cybercrime competences, the researcher predicts growth in the sophistication of anti-forensic tools aiming not just to conceal digital artifacts, but also to obstruct and paralyze cyber investigations, making law enforcement agencies waste as much time and resources as possible.

Perhaps surprisingly, in addition to the longitudinal spectrum of anti-forensics tools and creative techniques used to conceal digital evidence, procedural criminal law may likewise hamper digital forensics. The extent of hindrance depends on the jurisdiction. In Switzerland, for example, Article 248 of the Swiss Criminal Procedure Code of 5 October 2007, offers a fairly broad leeway to prevent evidence from rapid examination immediately after a search and seizure:

1. Records and property that according to the proprietor may not be searched or seized due to the right to remain silent or to refuse to testify or for other reasons must be sealed and may neither be inspected nor used by the criminal justice authorities.
2. Unless the criminal justice authority files a request for the removal of the seals within 20 days, the sealed records and property shall be returned to the proprietor. (Swiss Criminal Procedure Code, Art. 248)

Having no dramatic consequences for paper-based evidence that can be unproblematically examined any time after being sealed and confiscated, the foregoing provisions can create a major predicament for electronic evidence by excluding the possibility of live forensics, which may be indispensable to preserve the volatile data (as discussed in previous section). Resultingly, the prosecution's chances of finding incriminating artifacts or other valuable evidence are strongly diminished due to problems related to volatile data and ephemeral artifacts residing in RAM memory. The foregoing provision of Swiss Criminal Procedure Code illustrates that anti-forensic techniques are not necessarily limited to technical tools and methods, but may also involve abuse of the law.

In conclusion, the researcher predicts that both the frequency and sophistication of anti-forensics tactics will linearly increase. Whilst not all such tactics are fatal for digital forensics within criminal investigations, a considerable loss of time and resources for law enforcement agencies is guaranteed. Ultimately, the prosecution may despairingly abandon most digital investigations amid the increasing constraints on budgets, timelines, and qualified experts.

§ 2.6.5 Fake Evidence and the "Trojan Horse" Defense

The identities and whereabouts of perpetrators may be flatly unknown in some investigations, especially those implicating cybercrime (e.g., ransomware attacks) or computer-

enabled offenses (e.g., sexual crimes against minors entrapped on the Internet). The scarcely available digital evidence is commonly limited to scanty logs from breached systems or victims' devices, which may contain remote IP addresses, one-off email addresses, or the usernames of aggressors with whom the victim was interacting online before the crime. Such digital evidence requires a multiphase and technology-intensive investigation to unmask wrongdoers hiding behind chains of anonymous Virtual Private Networks (VPNs) or proxies, The Onion Router (TOR) networks, and one-off digital identities crafted to lure the victim into a trap (Europol, 2021). Particularly when the ephemeral smoke-screen systems are hosted in an elastic cloud, they can be shut down and unrecoverably destroyed in two clicks just after the completion of the crime, relying on the built-in features of modern CSPs enabling their clients to both deploy and destroy virtualized systems with lightning speed. Moreover, disposable proxies or VPNs may be deliberately located in hostile jurisdictions that will predominately refuse cross-border judicial assistance and cooperation, nullifying investigators' chances of clearing the crime. The jurisdiction-specific and cloud-specific problems of digital investigations are discussed in a detail in the upcoming sections.

Exacerbating the problem, cybercrime gangs incrementally sell access to compromised devices, systems, and even entire corporate networks on the Dark Web for as low as $10,000 per breached network, which may later be used to frame careless and unwitting enterprises by running sophisticated computer attacks or sending phishing and scam campaigns from their networks (Nichols, 2021). Cyber mercenaries and other sophisticated cyber-threat actors habitually purchase breached systems to reliably conceal their identities, sometimes purposefully framing innocent third parties. With the growing number of compromised police and law enforcement networks available for purchase on the Dark Web (Acharya, 2021; Resecurity,

2021), one may expect a steady increase of perfidious attacks originating from backdoored law enforcement infrastructures to frame the breached agencies and lead investigation into an impasse. Worse still, cyberattacks originating from law enforcement and other governmental systems may trigger severe consequences under international law and lead to spiraling political crises, as will be discussed in the next chapters.

Another potential investigatory nightmare is the so-called “Trojan horse” defense. Being less known in some jurisdictions than in others, this legal defense may be raised in criminal proceedings when incriminating electronic evidence is found on the suspect’s computer. The essence of this defense lays in the suspect’s blanket denial of being the author of the crime, shifting the blame to a Trojan horse or other type of malware present on the suspect’s computer (Bowles & Hernandez-Castro, 2015; Wilson et al., 2021). This defense has been used with a varying degree of success in a broad spectrum of criminal cases, spanning from child pornography possession to major cybercrime cases, including the criminal prosecution of Ross William Ulbricht in relation to the Silk Road online marketplace (Greenberg, 2015). Making the investigatory landscape even more uncertain and technically unsolvable, a group of researchers recently demonstrated that with specially prepared “Bad USB” attacks criminals may implant fake digital evidence on a computer—just by plugging a malicious USB key into the victim’s computer—that would be indistinguishable from authentic evidence, eventually leading to creation of erroneous forensic reports and eventual miscarriage of justice (Lawal et al., 2021). Analogously, criminals may also assert that they were victims of a Bad USB attack, leaving judges or jury unable to determine the truth. In summary, it is possible to image that one day, the falsifiability of seized electronic evidence may lead to persistent skepticism in the eyes of judges and jurors, who will simply ignore forensic reports produced by the prosecution or defense.

§ 2.6.6 XaaS and Digital Evidence Fragmentation

In all industries and sectors of the economy, the booming adoption and shift to the cost-efficient and scalable Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) business models have increased the fragmentation of electronic evidence across innumerable service providers (Gozman & Willcocks, 2019). A fusion of hardware, software, and SaaS providers morphs into Everything-as-a-Service (XaaS), creating a stark contrast with the previous state of affairs, whereby all digital evidence was collectable from a single source, such as a suspect's apartment or office. Nowadays, what is temporarily available on a suspect's device, for example, in RAM memory—as discussed in the data volatility section above—is likely to be permanently available in numerous remote systems operated by third-party service providers, ranging from small startups to tech giants from different countries and continents. The foregoing technical trends create an unprecedented fragmentation of digital evidence, whose physical location is highly diversified or is simply unknown, terminating the epoch of classic search and seizure investigations by law enforcement.

Technically, online "as-a-service" offerings range from simple storage services (e.g., Dropbox, Google Drive, or Microsoft OneDrive) to enterprise e-communication platforms that store confidential documents, billing information, and the business agendas of C-level executives, as well as operating voice and video calls (e.g., Microsoft Office 365 and Microsoft Teams). This is not to mention the even more complex systems designed to manage the entire enterprise sales cycle, enterprise-wide resource planning, accounting and billing, or vendor management. Eventually, end-user devices and smartphones gradually store less and less data, being used merely to connect to remote servers—where the data is actually stored—and becoming unattractive targets for search and seizure operations by law enforcement.

Consequently, a classic search and seizure procedure performed under a court-issued warrant may harvest considerably more evidence if directly conducted at the third-party service provider's premises—at least theoretically. In practice, however, insurmountable problems lay in the gigantic volume of data stored across countless interconnected servers, located in many countries and having proprietary or customized software or even tailor-made hardware, turning the search by law enforcement agents into an endless and cost-prohibitive exercise (Li et al., 2018). Furthermore, the problems of encryption elaborated in a previous section make searches of service providers pointless: the data is encrypted by default, whilst decryption keys may be stored in a foreign jurisdiction or may even be in the possession of a third-party supplier.

In sum, searching individual's devices and computers within criminal investigations is gradually becoming less productive. A massive shift to Microsoft Officer 365 has allowed users to store all their office documents in a cloud instead of on their hard drives. Predictably, law enforcement agencies have refocused their efforts on the voluntarily cooperation of service providers, seeking to obtain inculpatory evidence from them in a frictionless and agile manner (Tosza, 2021). This prima facie promising trend is, however, riddled with its own plethora of predicaments and complications, as discussed below.

§ 2.6.7 Jurisdiction Over Foreign-Stored Evidence

As discussed in the previous section, which outlined the last decade of technological globalization and decentralization, IT outsourcing and torrent-like migration to the public cloud has dispersed the data of companies and organizations around the globe in a manner that is virtually impossible to control, inventory, or map (Kleijssen & Perri, 2017). Whilst the leading Internet and cloud service providers usually allow their customers to preselect a geographical region in which their data will be physically stored, oftentimes, numerous third parties (e.g.,

backup or external IT service providers) can access the same data and copy it into to their own systems in foreign jurisdictions, creating a mosaiced data dispersion. The patchwork of data spraying is further aggravated by fourth parties, for example, backup providers of the third parties, located all around the world.

Multinational companies, global service providers, and supranational digital platforms such as Meta or Alphabet—better known for being the owners of Facebook and Google, respectively—have utterly convoluted data management strategies, interlacing vertical and horizontal layers or data streams. Frequently, their regional offices lack access to central systems, are unaware of their exact location, have no idea about their architecture and IT design, and may even be uninformed about their existence. Tellingly, Kleijssen and Perri (2017) point out that in a growing number of criminal investigations, it is technically unfeasible to ascertain where the requisite data is physically stored, as the data may be fragmented and continually fluctuate across several jurisdictions in a multicloud environment. Likewise, the question of who has the actual control of, or the access to, the data remains a mystery inside an enigma. Brown (2020) summarized the situation with piercing clarity:

> I would argue that traditional notions of territoriality applied to physical evidence are increasingly irrelevant [for electronic evidence]: when electronic evidence is involved and where a crime scene may well extend across multiple political borders; where counterparts may not be part of a trust-relationship or diplomatically predisposed to cooperate; and, when evidential data may be duplicated, relocated and routinely disseminated to additional jurisdictions at the press of a button. (Brown, 2020, pp. 431-432)

Criminal justice has traditionally been understood as confined by the physical borders of a sovereign state enjoying exclusive authority and virtually unrestrained power on its domestic territory, including soil, air, and water (Daskal, 2020). Historically, national criminal justice systems had no practical means or legal instruments to manage or direct criminal investigations in foreign states, but for certain narrow exceptions, for instance, those established by the virtue of multilateral or bilateral Mutual Legal Assistance Treaties (MLATs), wherein a foreign state may or may not respond to a request for assistance from another state in a cross-border criminal investigation (Osula, 2015). The conservative canons of criminal justice, entrenched in international law, undoubtedly politicize transborder criminal investigations, making their speed and efficiency almost entirely dependent on the comity of other states and their willingness to collaborate in cross-border investigations. Obviously, the global political crisis, unfolding at the time of writing, does not help with the existing frictions and barriers within foreign affairs. In continuation, the extraterritorial criminalization and prosecution of crimes committed abroad by nationals of the country—based on the nationality principle of jurisdiction—may also be mentioned among the exceptions, allowing domestic justice to penalize the foreign behavior of its nationals; however, its influence on cross-border search and seizure of digital evidence is infinitesimal (Megret, 2020). Examples of existing legislation on cross-border investigations, allowing for remote searches and seizures under certain conditions, are discussed in the next chapter of this dissertation.

Questions of territoriality and state jurisdiction over foreign-based electronic evidence has always been an utterly complex legal issue, involving the rapidly evolving national jurisprudence, the inching development of international law fostered by ratifications, implementations or amendments of international treaties, and the multidisciplinary questions

involving politics, public policy, and diplomacy. Whilst new theories and pathbreaking approaches to tackle the issue of territorial jurisdiction in cybercrime prosecution emerge (Li & Qin, 2018), the question of jurisdiction over foreign digital evidence is still largely unsettled and remains the inexhaustible source of problems for law enforcement (Daskal, 2020). Unwarranted transborder seizures of electronic evidence may infringe the inviolable principle of territorial sovereignty, which is deeply rooted in international law, and may trigger serious legal ramifications and erode diplomatic relationships between countries (Osula, 2015). Similarly, the legality of seizing data hosted abroad but accessible locally (e.g., downloading incriminating documents from a foreign-based server by using an active login session from a seized laptop) remains largely unsettled across jurisdictions and may impact the eventual admissibility of electronic evidence in a national court. In continuation, even when foreign evidence is obtained while rigorously following international law, its fate in national courts remains uncertain. Illustratively, in the European Union, although Member States' legislation predominantly converges on the admissibility of electronic evidence lawfully obtained abroad via MLATs or similar instruments in cross-border criminal investigations, not all EU countries have codified this principle into their statutory law (EU SIRIUS, 2021), giving a rise to procedural ambiguity and uncertainty.

The Budapest Convention on Cybercrime of 2001, which has been signed by 66 states at the time of writing (Council of Europe, 2022), is probably the most important international treaty designed to combat cybercrime and computer-enabled offenses. In addition to the enhancement and harmonization of national cybercrime legislation across signatory states, faster investigations, and more successful prosecution of computer-enabled crimes, the Convention comprehensively addresses mutual legal assistance between the parties to the it within

transborder criminal investigations. The legal assistance encompasses such essential elements as the extradition of criminals, preservation of digital evidence upon request, disclosure of intercepted communications and stored data to competent foreign agencies, and establishment of a 24/7 point of contact—within each country—that would operate in a seamless collaboration with other states under the provisions of the Convention.

Despite its unquestionable power and the associated benefits for cross-border investigations of computer-enabled crime, the Convention has some palpable drawbacks. Firstly, at the time of writing, China, Russia, and most other developing countries have not signed the Convention, leaving the signatories with no redress when digital evidence is stored in a non-signatory state. Secondly, the language of a significant number of articles in the Convention is conceptually debatable, equivocal, or ambiguous, leaving the signatory countries a wide leeway to construe and argue for its own meaning of the text in divergent and inconsistent ways (Blažič & Klobučar, 2020). Likewise, practical enforcement mechanisms in relation to the mutual legal assistance are missing in the Convention, leaving parties thereto without recourse in the case of non-compliance by another party (Verdelho, 2019). Thirdly, despite the recent adoption of the Second Protocol to the Convention, which aims to address the growing concerns over slow and inefficient interstate collaboration through the implementation of expedited and emergency data request mechanisms (Daskal & Kennedy-Mayo, 2020), the Protocol has been signed by only 22 states at the time of writing (Council of Europe, 2022a). Fourthly, the Convention is naturally of no help when the location of digital evidence is unknown or when the evidence is encrypted. Finally, in view of the doubts cast by the European Data Protection Board (EDPB) over the Protocol's compatibility with the EU GDPR and the fundamental privacy protection

requirements (European Data Protection Board, 2021), the further operationalization of the Protocol languishes in obscurity.

In contrast to the courteous but unhurried negotiations under MLATs, a more efficient, straightforward, and seamless approach has been proposed by the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018. Among other things, this Act purports to streamline bilateral cross-border access to digital evidence between the United States and foreign states having Executive Agreement under the provisions of the Act. This novel apparatus of the transborder legal assistance enables law enforcement agencies, when investigating serious crime, to bypass the protracted MLAT mechanisms and to request electronic evidence from foreign service providers directly, with the same effect and binding power as if they had reached out to domestic providers. There are some notable exceptions thereto, for instance, foreign data requests targeting the data of a U.S. resident or citizen must still follow the traditional MLAT avenue, whereas reciprocal protection is granted upon other states in relation to their residents (Daskal, 2019), thereby shrinking the perimeter of Act's applicability. This is likely one of the reasons why legal scholars have cautioned that the benefits granted to law enforcement under the Act are not as revolutionary as initially contemplated by the U.S. lawmakers and then claimed by the U.S. Department of Justice (DoJ) (Cochrane, 2021). Furthermore, at the time of writing, Executive Agreements were established only between the United Kingdom and Australia (Department of Justice, 2022). Likewise, taking into consideration that the two formidable guardians of the European privacy regime, namely the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), jointly raised doubts over the adequacy of privacy protection under the CLOUD Act and thus its potential incompatibility with the EU GDPR (EDPB & EDPS, 2019), so an Executive Agreement between the United States and the

EU seems quite unlikely to take place in a near future. In sum, whilst being a palpable improvement of the archaic MLAT mechanisms, the CLOUD Act is not a panacea and is, likewise, toothless when dealing with the concomitant challenges of criminal investigations in cyberspace (e.g., strong data encryption discussed in a detail in previous sections).

On the one hand, one can evidently observe the intensifying efforts of many states to create a congruent, efficient, and frictionless MLAT framework to lawfully obtain foreign-stored electronic evidence when it is technically feasible to do so. One laudable example of an agile, effective, and sustainable public–private collaboration is the amplifying success of the EU-wide SIRIUS public–private platform, created by the Europol and Eurojust for electronic data exchange between law enforcement agencies and online service providers. Similarly, the increasing success of the European Investigation Order (EIO) in the EU (Blažič & Klobučar, 2020) and the currently pending proposal for the European Production Order (EPdO) and the European Preservation Order (EPsO), which are specifically designed for electronic evidence (Tinoco-Pastrana, 2020; European Commission, 2018), serve as laudable examples of the cross-jurisdictional harmonization of procedural criminal law and fluid interstate cooperation between law enforcement agencies. On the global and supranational level, the United Nations Office on Drugs and Crime (UNODC) designed and proposed a model of a transcontinental Data Disclosure Framework (DDF) that may inspire sovereign states to enter into multilateral or bilateral treaties tailored both to protect individual privacy and to bolster the effectiveness of criminal investigations (UNODC, 2021).

One the other hand, privacy advocates continually adduce reasonable, albeit often one-sided, arguments against the facilitation of cross-border collaboration in digital investigations. Illustratively, the European Digital Rights (EDRi) association released a comprehensive report

coauthored by 13 other non-profit organizations defending civil rights; the report castigated the proposed draft of the EU e-Evidence Regulation, which was actually supposed to operationalize the EPdO and EPsO mechanisms described above (European Digital Rights, 2021). The report also loudly sounded the alarm over possible violations of human rights and freedoms, spanning from the right to a fair trial to the protection of journalistic sources. Sadly, the proposed reforms of the Regulation, such as mandatory notification of the suspect, whose data was disclosed in a cross-border request, negate most of the benefits contemplated under the Regulation. Eventually, the chances of unhindered and efficient cross-border collaboration, in relation to digital evidence stored in foreign jurisdictions, rapidly fade (Propp, 2022). Furthermore, many countries and private enterprises are reluctant and hesitant to cooperate in criminal investigations for a multiplicity of presumably valid reasons, aggravating the already complicated position of law enforcement. Some countries still have no MLAT mechanisms whatsoever and rely on obsolete liaisons by diplomatic channels. Others have cumbersome and protracted MLAT agreements that visibly cannot help in cross-border investigations involving volatile digital evidence. Even worse, amid the ground-trembling events like Brexit and the unfolding geopolitical crisis of 2022, even more divergency and disaccord among the states or states-wide unions, such as the EU or the BRICS (Brazil, Russia, India, China and South Africa), may have a persistent chilling effect on the interstate collaboration within cross-border investigations of serious and organized crime.

A comprehensive scholarly literature review performed by Casino et al. (2022) cogently summarizes the key problems discussed in this section. The scholars adduce, among other things, the following barriers to cross-border criminal investigations involving electronic evidence: (i) “[t]imely collection, analysis and sharing of evidence”; (ii) “[l]ack of harmonisation in rules of

admissibility of criminal evidence and prosecution"; and (iii) "[i]ncompatibility conflicts between jurisdictions that may violate procedural rights and safeguards" (Casino et al., 2020, p. 8, "Table 3: High level abstraction and description of the challenges identified in the literature"). As demonstrated above, at the time of writing, no globally accepted legal basis exists for accessing foreign-stored electronic evidence, leaving law enforcement agencies in a legal vacuum. Criminals are well aware of the problem and deliberately use foreign service providers from countries known for poor collaboration with their neighbors. Whilst some rudimentary mechanisms exist to lawfully obtain foreign evidence, they commonly lack generalizability, predictability, and rapidity that are indispensable for efficient investigations in cyberspace. In Chapter 3, the researcher discusses several creative solutions to transborder investigations of serious and organized crime that are incorporated into national legislation on lawful hacking.

§ 2.6.8 Broken Communications With Service Providers

In response to the multifaceted pitfalls of MLATs discussed above, law enforcement agencies have started to contact service providers directly, trying to obtain digital evidence faster and without bureaucracy. Whilst being heavily dependent on the jurisdiction and influenced by international treaties in place or by the lack thereof, the informal cooperation of service providers with law enforcement detectives may be an attractive way to obtain digital evidence within criminal investigations (UNODC, 2019). For instance, in the United States, service providers are expressly authorized by the Electronic Communications Privacy Act (ECPA) of 1986 to respond to lawful information requests by voluntarily providing digital evidence (e.g., subscriber data) to foreign law enforcement agencies from jurisdictions where the service provider operates or stores the data in question (Swire et al., 2016; Kleijssen & Perri, 2017). Similar legislative regimes prevail in European countries (Blažič & Klobučar, 2020), though not all EU member

states have codified this principle into their national law, leaving the legality of transferring data in response to lawful requests from foreign law enforcement agencies in judicial limbo (EU SIRIUS, 2021).

Likewise, depending on the factual context and implicated jurisdictions, direct collaboration with service providers may be even thornier and more grueling than the traditional MLAT route is. The reality is oftentimes saturated with country-wide and provider-specific obstacles of a substantive and procedural nature (Gutheil et al., 2017). Illustratively, Apple and Facebook have country-specific policies on whether and how to handle law enforcement requests, depending on the nature of the information sought, the gravity of the offense, and the justification for disclosure (T-CY Cloud Evidence Group, 2016a). Evidently, such policies are impacted, inter alia, by foreign politics and other nontechnical matters. Moreover, unpredictable capriciousness among service providers, sometimes verging on arbitrariness and abuse of law, may exacerbate direct collaboration and undermine its future potential:

> Provider policies are volatile and lack foreseeability for law enforcement as well as customers. Service providers may change their policies unilaterally at any time and without prior notice to law enforcement. Adding to this, policies and practices not only differ widely between providers but also with respect to different Parties to the Budapest Convention. One provider may respond to many requests from one country but to none or a few requests only from another country, while the practices of another provider may be exactly the opposite. (T-CY Cloud Evidence Group, 2016a, p. 22)

Interestingly, the responsibility for broken communications is attributable not only to service providers: the recently surveyed providers complained about requests coming from law enforcement agencies having (i) an “absent or incorrect” legal basis, (ii) “[p]rocedural mistakes

according to [service provider] requirements," and (iii) "[o]verly broad [data] request[s]," naming those inaccuracies as among the key reasons they have to regularly refuse to fulfill data disclosure requests coming from abroad (EU SIRIUS, 2021, p. 61). Remarkably, service providers also cited a large volume of misaddressed requests, wherein police officers confused one service provider with another. Additionally, according to the surveyed service providers, a considerable number of requests from law enforcement agencies contained illegible, insufficient, or incomprehensible user identifiers, as well as ambiguous or inflated justification for emergency data requests, eventually frustrating the rapid provision of the requested data. Notwithstanding the foregoing, justified and clear data requests seeking only subscribers' information are likely to be swiftly and unproblematically addressed, whilst stored data production or communication interception requests may literally take years, only to eventually end up at a procedural impasse. Analogously, the provision of non-resident information is usually a less cumbersome and less hostile process, being intrinsically less confrontational with national privacy-protection laws, compared to the provision of resident data, which is increasingly being provided solely in response to a domestic court order or warrant.

Vermeer et al. (2018) indicated that a lack of special training and technical knowledge among law enforcement officers, combined with the unique IT architectures of service providers, negatively influences their already-fragile relationships, pushing them towards increasing adversity. Technically, some cloud vendors simply do not store logs of specific events due to their voluminosity and, thus, they cannot help investigators even if they want. Sometimes it is truly impossible to map a specific user's identity onto certain activities happening within automatically orchestrated Docker containers in a user's private cloud environment. Likewise, service providers frequently cannot deliver raw binary data in a readable Microsoft Excel or PDF

file—as requested by technically inexperienced law enforcement officers. Procedurally, both service providers and law enforcement agencies complain about the inconsistent processes and accompanying paperwork in relation to data production requests and responses. Sometimes, busy police officers may mechanically send a boilerplate request by fax to the service provider's central number and expect an instant response; for their part, some service providers lack any internal policies on collaboration with the authorities, handling incoming requests in an aleatory and unpredictable manner (EU SIRIUS, 2021).

In conclusion, fundamentally incompatible legal systems, opposing public policy regimes, rapidly evolving case law, and newly enacted privacy legislation mercilessly torpedo the predictability of public–private collaboration in cross-border and even domestic crime investigations. Worse, even when the legal landscape is homogeneous and favors frictionless collaboration, the non-interoperability of modern technologies, lack of technical training, and unprecedently complex IT ecosystems annihilate the benefits of direct collaboration with third-party service providers. Accordingly, law enforcement officers can rarely rely on service providers for actionable support in investigations of serious and organized crime.

§ 2.6.9 Data Retention Policies of Service Providers

In continuation of the previous section, the rallying privacy protection legislation is another trend that—somewhat surprisingly—crushingly frustrates criminal investigations. While national law enforcement agencies are typically exempt from national legislation in relation to privacy protection, service providers are not. The intersection of legislation on mandatory data retention by telecoms and some service providers, initially enacted to assist law enforcement agencies in criminal investigations, may likewise be at odds with emerging privacy protection laws and may even be invalidated for that very reason (Rojszczak, 2021). For instance, the right

to be forgotten has spread from the European Union to other countries and continents, giving users comprehensive control over their personal data processing and the right to request data controllers (i.e., service providers) to erase their data (Casino et al., 2022). Whilst service providers may, of course, have a legitimate interest in storing some personal and related data for at least as long as prescribed by national data retention laws, the remainder of user data should, arguably, be rapidly deleted upon a user's request. Some providers retain user data, arguing that they have a legitimate interest in preventing and investigating fraud by doing so, however, how resilient their reasoning will turn out to be in court is largely uncertain.

Under the mushrooming privacy laws and regulations, in addition to the exercisable right to be forgotten, data controllers (i.e., service providers) are normally required to store personal data for only as long as legitimately needed, even if a user does not request deletion. Without delving into the legal complexities of whether, when, and for how long service providers may have a prepondering legitimate interest in preserving the personal information of data subjects—for example, as mentioned in the previous paragraph to comply with national data retention law (EU SIRIUS, 2021)—it becomes self-evident that privacy-protection laws may unwillingly hinder and obstruct criminal investigations in cyberspace. Being overly intimidated by the soaring fines and severe penalties for violations of data retention provisions imposed by privacy protection laws, service providers are rather inclined to delete increasing amounts of personal data, eventually having almost nothing to share with police officers when required to do so within a criminal investigation. Conversely, as remarked by Casino et al. (2022), privacy legislation also has a positive effect for digital investigations. Strict requirements in relation to personal data localization within geographical boundaries (e.g., under provisions of the EU GDPR) may simplify and accelerate criminal investigations within the EU by centralizing

personal data on European soil, where EU law enforcement agencies may extract it with comparative ease. Notably, the unfolding privacy battle is not exempt from the other challenges described in this chapter, particularly that of encryption.

Tellingly, the commencing data retention crisis is already observed by law enforcement professionals. A recent survey, conducted among law enforcement agencies and judicial authorities within the EU, found 57.1% of respondents to believe that "[d]ata retention periods are too short or non-existent," whereas 34.7% also complained that "[service providers] usually take too long to reply to direct requests" (EU SIRIUS, 2021, p. 37). Consequently, when a data production request is finally reviewed and approved by a service provider, the data in question no longer exists, negating all efforts made to acquire it. Respondents of the same survey also mentioned that certain service providers still have no enterprise-wide data retention framework, turning data availability into a gamble. Additionally, despite the increasing acceptance of data preservation requests by service providers, if the requested data is available under the provider's data retention regime, those requests are handled in contrastingly divergent manners and at a different speed, varying among service providers (T-CY Cloud Evidence Group, 2016a). In sum, contemporary privacy legislation, namely its data retention rules and requirements, is a nascent but already-formidable opponent of digital investigations of serious and organized crime.

§ 2.6.10 Notifications by Service Providers

In addition to the grim labyrinths and problems concerning public–private cooperation in crime investigation discussed above, service providers may notify their customers about data disclosure to law enforcement agencies. Needless to say, the impact of such notification can be disastrous and, even fatal, for the outcomes of investigation: seasoned wrongdoers will swiftly abscond to overseas jurisdictions and take supplementary precautions to avoid leaving digital

footprints in the future. Illustratively, Google, whilst being one of the most frequent recipients of data disclosure requests from law enforcement agencies (EU SIRIUS, 2021), readily collaborates with authorities by providing at least "some data" in 83% of requests from law enforcement agencies. However, Google also commonly notifies its users before handing their data to authorities to allow them to contest the disclosure in court (Bhuiyan, 2021). Most other U.S.-based tech giants, including Facebook, Twitter, Apple, and Microsoft, likewise send notifications to their users in a considerable number of cases, as well as publish annual transparency reports to elaborate on their cooperation, or lack thereof, with domestic and foreign law enforcement agencies (T-CY Cloud Evidence Group, 2016a).

To remediate the negative impact of notification, the framework by the UNODC (2021) suggests that service providers should assess their rights and duties under applicable law and then develop a thorough notification policy that would fairly balance the legitimate interests of users with the utilitarian needs of criminal justice and society. For instance, once the investigation ends or the surveilled user is arrested, questioned, and released by police, the notification may generally be sent, as no reasonably foreseeable risks to the investigation remain. Likewise, law enforcement agencies—when so is necessary—are recommended to expressly and conspicuously mention in their data production requests that any notification to subscribers may jeopardize the investigation and, hence, should not be given unless mandated by local law (UNODC, 2021). Unfortunately, until most developed countries agree on some form of uniformed principles of cross-border investigations and then enact compatible national laws and procedural rules to govern access to foreign digital evidence and the disclosure thereof, these notifications will continue poisoning digital investigations. In light of the currently incompatible privacy protection frameworks and the polarized underlying philosophies in the United States

and Europe, the near-term prospect of so-called defragmentation of national laws, unfortunately, seems utopic.

§ 2.6.11 Public Cloud-Specific Problems

Whilst offering unsurpassable scalability, agility, and cost-efficiency—compared to on-premise infrastructure—the modern public cloud creates unprecedented technical and operational complexity. The spiraling sophistication of cloud architecture, combined with the ongoing evolution of cloud platforms and services, requires special skills and technical training from digital investigators from law enforcement agencies, whose cloud-related knowledge commonly ranges from non-existent to modest (Olber, 2021). The three titans of the modern public cloud empire—Amazon AWS, Google Cloud Platform, and Microsoft Azure—offer over 100 cloud services each. The cloud service span from the automation of machine learning tasks and blockchain management to e-commerce fraud detection and business workflow orchestration, let alone the abundant variety of classic services for data processing and storage, such as scalable virtual machines, network load balancers, or elastic block storage (Jones, 2021).

As summarized by Brandao (2019), directly consumable cloud services, mostly those related to processing or storage of data, can be categorized into three principal models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Whereas the SaaS model provides the least degree of control and customizability to customers, the IaaS model offers almost unlimited control over cloud assets, which is, however, accompanied by the responsibility to manage and secure those assets. The PaaS model is somewhere in between the SaaS and IaaS approaches. There are also ancillary hybrid and mixed models for various cloud managements tools or applied services, ranging from automated billing control to event-driven software code execution in a serverless environment (also known as

Function-as-a-Service [FaaS]) and managed Continuous Integration and Continuous Deployment (CI/CD) pipelines for agile software development and testing. The highly volatile cloud environment oftentimes erases the demarcation line between stored data and data in transit, leaving puzzled law enforcement investigators guessing what type of warrant is actually required to get the data. Procedurally, the externally managed nature of cloud services creates judicial ambivalence and an enigma concerning whether a cloud provider itself or its customer shall actually produce the evidence. Despite the increasing number of available trainings and certifications on cloud forensics (SANS, 2022), most are primarily focused on Incident Response and Digital Forensics (DFIR) methodologies for security analysts uninvolved in any legal or judicial proceedings. Another common pitfall of the existing cloud training is its intrinsic design, which is mainly tailored for cloud infrastructure owners or operators, who possess unlimited access to and control over their cloud environments, while the external prospective of law enforcement agencies is largely unaddressed.

To continue, the jurisdictional impasse over digital evidence discussed in the previous section of this chapter is particularly onerous in a cloud environment, considering that cloud data may simultaneously reside in several sovereign states unbeknownst to either the cloud provider or to the customer, let alone to law enforcement agencies. Multicloud environments, which offer advanced resilience by mirroring the data across several synchronized cloud providers, add a persistent connotation of enigmatic mystery into the question of location and jurisdiction over the data. Interestingly, the Cloud Evidence Group of the Cybercrime Convention Committee (T-CY) even theorized that unscrupulous CSPs may purposely move data across different countries to hinder criminal justice investigations in bad faith:

> It is often not obvious for criminal justice authorities in which jurisdiction the data is stored and/or which legal regime applies to data. A service provider may have its headquarters in one jurisdiction and apply the legal regime of a second jurisdiction while the data is stored in a third jurisdiction. Data may be mirrored in several or move between jurisdictions. If the location of data determines the jurisdiction, it is conceivable that a cloud service provider systematically moves data to prevent criminal justice access. (T-CY Cloud Evidence Group, 2016, p. 15)

Unsurprisingly, some members of the law enforcement community perceive public cloud providers to be "not law-enforcement friendly," suggesting that certain providers may even be deliberately uncooperative and malignantly sluggish, vigorously defending their clandestine clients, who actually represent their source of revenue (Dees, 2018). The negative denotation of the cloud within criminal investigations is also hyperbolized by the general lack of technical knowledge and understating of the evolving cloud technologies, applicable law, and existing collaboration mechanisms among prosecutors, police officers, and even magistrate judges. The consequence is that the emerging and fairly efficient mechanisms of cross-border cooperation between state law enforcement agencies, including but not limited to novel mechanisms specifically designed to obtain cloud-stored data or the 24/7 points of contact established under the Budapest Convention, remain largely underused and ignored by law enforcement agencies and other authorities (Olber, 2021).

In the modern multicloud environment, criminals may store their files, install dedicated email or instant messaging servers in a cloud to avail themselves of the numerous options of strong turnkey encryption available in the cloud environment. Legitimately rented cloud infrastructure with strong data encryption both at rest and in transit is actually a perfect place to

hide something illicit, being a needle in a haystack. Aiming to safeguard the privacy and data confidentiality of their enterprise and governmental customers, most cloud service providers offer military-grade encryption with cryptographic keys stored in physically isolated Hardware Security Modules (HSMs), making them technically non-interceptable and physically unextractable (AWS, 2022). With properly implemented and hardened encryption in a cloud environment, even if equipped with a warrant or court order, neither the CSP nor law enforcement agencies will ever be able to decrypt the wrongdoers' data. Another inherent problem with the cloud environment is cloud-wide virtualization, as most multilayered cloud services run on an exhaustively virtualized and ephemeral infrastructure: once a specific service or cloud instance is terminated by the customer, all allocated storage resources will be instantly reassigned to another customer, irretrievably flushing all the data (T-CY Cloud Evidence Group, 2016; Srivastava & Choudhary, 2021; Syed & Anu, 2021).

Modern cloud forensics differs remarkably from traditional digital forensic science. When dealing with the cloud, cyber detectives virtually never have physical access to the underlying hardware, which is dispatched in multitenant and multi-datacenter environments across different cities, countries, or even continents (Freet et al., 2015). Therefore, traditional forensics that involves hardware seizure and subsequent inspection is rarely, if ever, available in a cloud environment. Notably, powerful cloud-native tools are made available by leading CSPs to streamline the event-driven, periodic, or manual snapshotting of virtual machines, virtual storage drives, virtual networks' traffic, or even the RAM of virtual machines for subsequent investigation. However, such tools, are not enabled by default, require advanced technical skills to set up and utilize, and most importantly, are not designed for external criminal investigators, instead targeting cloud customers and their internal DFIR teams having full access to the cloud.

Moreover, despite the cutting-edge automation of cloud DFIR capabilities, available as separate cloud services or tools, the vast majority of them are very specific to a cloud provider and, thus, require custom knowledge and experience from investigators. This is not to mention that such tools are rapidly evolving and require continuous training from cloud investigators. Similarly, whilst the modern-day cloud environment usually provides expanded logging capabilities and more detailed events in the logs—compared to traditional on-premises environments—the cloud logs are commonly disabled or minimized by default to save storage costs. Cloud logs equally require CSP-specific knowledge to be successfully utilized in investigations, leaving many law enforcement agents disarmed. Additionally, in practice, for cost-optimization purposes, most logs are stored for less than six months, unless strict compliance requirements dictate otherwise. Hence, unless law enforcement agents manage to team up with a cloud customer's DFIR team having access to the sought electronic evidence, it is unlikely they will even notice any palpable benefits of cloud forensics tools and services. In sum, if sophisticated wrongdoers rent cloud IaaS services themselves to process their own data and communications in a secure and encrypted manner, law enforcement will likely encounter an insurmountable stone wall of technical problems even in trying to extract a single byte of digital evidence.

Manral et al. (2019) conducted a comprehensive survey of cloud-specific challenges to digital investigations, which cogently classified five main challenges to cloud forensics: (i) evidence identification; (ii) evidence collection; (iii) evidence preservation; (iv) evidence examination and analysis; and (v) evidence reporting and presentation. The evidence identification problem originates from the highly fragmented and transient distribution of customer data across cloud data centers in foreign countries, which also gives rise to the knotted dilemma of jurisdiction discussed above. Next, the evidence collection challenges include such

major difficulties as cloud encryption, which increasingly becomes enabled by default, as well as CSP-specific architecture requiring dedicated human expertise. Especially pronounced in the contemporary cloud environment, the issues of evidence preservation encompass the volatility and ephemerality of electronic evidence, namely when dealing with the chain-of-custody and evidence isolation requirements in a multitenant cloud environment. Finally, the issues of evidence examination and analysis involve the heterogeneity of available cloud DFIR tools and services with significant dissimilarities and technical nuances across different cloud service providers, which also may use distinctive log formats and retention periods (Manral et al., 2019; Fernandes et al., 2020), thereby complicating the eventual preparation of forensic reports for court proceedings. As demonstrated above, in the investigation of serious and organized crime in a modern cloud environment, the headaches of law enforcement become migraines.

§ 2.6.12 Mobile-Specific Problems

Mobile phones are an inalienable part of everyone's daily personal and professional life, being used by virtually all people of all ages, professions, and social statuses. Unsurprisingly, modern smartphones have naturally become crucial for criminal investigations, storing pivotal electronic evidence of all types of serious crimes, from isolated armed robbery to disastrous cases of mass-murder, as with the infamous San Bernardino terrorist attack, which precipitated a general awareness of the challenges commonly faced by law enforcement in relation to the collection of inculpatory evidence from suspect's mobile devices (Cahyani et al., 2016). Whilst a seized mobile device may be metaphorically compared to an Ali Baba cave full of incriminating digital evidence, it also brings its own problems and difficulties to law enforcement investigations.

Back in 2013, digital evidence seized from then-basic smartphones was already crucial in a growing number of judicial proceedings, being leveraged to prove suspects' innocence or guilt (McMillan, Glisson, & Bromby, 2013). In its landmark *Riley v. California* (2014) decision, the Supreme Court of the United States unanimously held that a mobile phone search incidental to arrest requires a warrant, reversing all preceding rulings of lower courts and setting a new privacy doctrine in the country (Electronic Privacy Information Center [EPIC], 2014). The nine Justices emphasized that modern smartphones contain an all-inclusive spectrum of personal and professional information, including the most sensitive and confidential details of everyday life, which merit the highest degree of protection. In its more recent decision—*Carpenter v. United States* (2018)—the Supreme Court coherently augmented and enhanced the protection of mobile privacy by ruling that requesting Cell Site Location Information (CSLI) likewise requires a warrant (Liptak, 2018). Unfortunately, albeit quite foreseeably, savvy criminals perfidiously abuse modern privacy protection regimes to further their nefarious crimes with growing impunity. Interestingly, the legal aftershock of the dramatic San Bernardino case is far from being over: Apple is currently suing the cybersecurity vendor that reportedly helped the FBI to unlock the iPhone of the attacker (Nakashima & Albergotti, 2021). In a similar move, WhatsApp has filed a lawsuit against the NSO Group, discussed in the first chapter of this dissertation, for the alleged hacking of its instant messaging application (Penney & Schneier, 2022). The outcomes of both cases may have serious ramifications for law enforcement agencies relying on third parties within criminal investigations, leaving them with two unpromising alternatives: to either spend tens of millions of taxpayer dollars on the in-house research and development of governmental zero-day exploits and spyware or, in sharp contrast, do nothing and implicitly condone the unbridled proliferation of serious crime amid a lack of investigatory resources. The

usage of zero-day vulnerabilities by law enforcement agencies, within investigations of serious and organized crime, is discussed both below and in Chapter 4.

Whilst the layperson generally lacks awareness of the readily available security-hardening features and advanced privacy-protection options offered abundantly by the leading mobile phone manufacturers (Pawlaszczyk, 2022), organized crime excels in misusing these vendor-supplied security controls to make mobile forensics a fruitless process for law enforcement. Strong encryption—enabled by default—is, arguably, the most formidable barrier for mobile investigations (Fukamia et al., 2021). Differently from most laptop or desktop computers, which commonly rely on a comparatively unsophisticated architecture of full-disk encryption (Tan et al., 2020) that is infrequently enabled by default, modern smartphones leverage strong, multilayered encryption, as well as the physical isolation of the encryption keys, making attacks on data extraction and decryption virtually impossible. Worse still, mobile encryption is now predominately enabled by default and does not require any special knowledge or skills to be activated. Illustratively, the built-in anti-bruteforcing protection available on both Android and iOS devices permits smartphone users to automatically flush all data from their smartphone after 10 incorrect passcodes are entered. The situation is further exacerbated by user-friendly remote wiping mechanisms, which are, of course, valuable to protect legitimate users when their smartphone is stolen, but are also misused by criminals to paralyze investigations of seized devices. In an attempt to finally balance legitimate mobile privacy with the prosecutorial needs, Savage (2018) invented a novel privacy-preserving approach to mobile passcode resetting by allowing a device-unique password reset to be performed by manufactures upon receipt of court order. The approach proposed by Savage does not rely on a universal backdoor that would automatically unlock any device, but rather on a manually activatable and device-specific

password reset that would neutralize the perils of mass backdooring that are discussed below. However, this wise approach would require industry-wide changes to mobile firmware and possibly hardware and, thus, is unlikely to materialize in the near future.

The contemporary multivendor environment of the global mobile phone market, wherein each mobile phone commonly has dozens of externally developed apps, makes mobile investigations even more taxing (Li et al., 2018). An additional layer of encryption is usually integrated into mobile applications on top of mobile operating system encryption, both protecting the device-stored app's data and its data in transit, oftentimes with the E2EE encryption discussed in the previous section. Most mobile applications such as instant messengers or password manager apps, which actually represent the biggest interest for law enforcement investigators, usually use their own data encoding and storage formats in addition to strong encryption enabled by default, making evidence acquisition a time-consuming process even if smartphone is unlocked. Additionally, vital data may be securely stored in a cloud, releasing the parade of cloud horrors discussed in the previous section. Self-destructing and automatically disappearing messages, likewise explored above, fiercely push the cumulative value of mobile investigations toward nullity.

Whilst numerous creative loopholes exist to bypass mobile encryption, ranging from trivial passcode guessing or bruteforcing attacks to acquisition of a mobile device's unencrypted backup from a desktop computer or Apple's iCloud (Menn, 2020), they are mostly exploitable against unexperienced users and rarely work against crafty criminals with properly hardened smartphones (Herrera, 2020). Likewise, simple passcode bypass tricks, such as bringing an Android device with enabled "Smart Lock" option into a trusted place, are likewise toothless against members of transnational criminal syndicates and organized crime gangs, who are far

from being naïve, technically uneducated, or careless. Eventually, a properly hardened mobile phone, running on the most recent version of hardware with up-to-date firmware, becomes an unassailable bastion for digital investigators from law enforcement agencies.

More advanced mobile investigation techniques include hardware-level Joint Test Action Group (JTAG) and chip-off data acquisition or the exploitation of manufacturer-specific hardware and software vulnerabilities. While these techniques may be fruitful under a narrow set of circumstances, they all have considerable implications for the integrity and further preservation of the extracted evidence in conformity with applicable chain-of-custody requirements (Fukamia et al., 2021). Likewise, advanced attack vectors are predominantly vendor-specific, broadly varying from one mobile operating system version to another, as well as the underlying hardware of the device. Fukamia et al. (2021) highlighted that novel investigation techniques, such as side-channel attacks, fault injection, or System-on-a-Chip (SoC) reverse-engineering, are promisingly potent for mobile investigations, however, at the time of writing they are equally prone to the foregoing weaknesses, being unable to synthesize a reliable, cost-efficient, and universal mobile forensics methodology for criminal investigations.

Another distinguishable impediment to efficient, rapid, and cost-effective mobile forensics stems from insufficient training and lack of cyber detectives with technical skills in mobile investigations. Modern mobile forensics requires a multifaceted set of advanced tech skills to perform forensically sound data acquisition, designed to properly extract digital evidence adducible in court. For instance, reverse engineering and mobile programming, proficiency in using mobile forensics tools, good understanding of mobile operating systems, as well as the architectures of various security mechanisms and proprietary mobile encryption frameworks are just a tip of the contemporary mobile forensics iceberg (Reedy, 2020; Humphries

et al., 2021). In view of the relentless technical progress and continuous evolution of mobile security technologies, police investigators are to regularly undertake expensive trainings on mobile forensics, which may be cost-prohibitive for small law enforcement agencies or agencies from developing countries.

Alarmingly, only major law enforcement agencies from a few wealthy megapolises or countries can afford to pay seven-figure amounts to selectively unlock mobile devices by exploiting zero-day vulnerabilities (Betschen, 2018). Those agencies may even exert pressure on the mobile device manufacturers, demanding assistance or at least a noninterference by pausing the implementation of anti-forensics mechanisms (Menn, 2020). At the same time, less generously funded agencies are discriminatively excluded from this privileged circle of opportunities. Predictably, the opponents of lawful hacking frequently invoke impressive and eye-catching statistics from wealthy law enforcement agencies in relation to successful unlocks of seized smartphones by police investigators. For instance, some invoke the strikingly high 60% success rate of device unlocks mentioned in the 2019 report by the New York District Attorney's Office (Hewson & Harrison, 2021). The situation is, however, far from being simple and straightforward as alleged by the opponents of lawful hacking. Firstly, in isolation from other data and numbers, such statistics may be substantially misleading. For instance, it is unclear how many of the unlocked smartphones were actually implicated in serious crimes—both in absolute numbers and in percentage—compared to all other unlocks. Secondly, a comprehensive nation-wide statistic will likely provide a contrastingly lower success rate, especially from smaller cities and rural counties. Thirdly, those numbers should be analyzed through the prism of serious crimes that could have been cleared but were not due to the unlockable mobile devices. Moreover, the number of smartphones belonging to organized crime gang members that could

not be found or seized and, thus, were never investigated should be considered as well. Eventually, a deep dive into the numbers will likely demonstrate that even the most powerful law enforcement agencies cannot afford to streamline smartphone unlocks when investigating serious and organized crime, let alone smaller agencies or regional units.

In sum, compared to desktop computers or laptops, the mobile device attack surface and the available software and hardware attack vectors against smartphones are considerably smaller. Competing mobile manufacturers strive to provide their users with the strongest protection of privacy and security, and organized crime is certainly one of the beneficiaries of this otherwise praiseworthy trend. That is not to suggest that mobile security or privacy should be diminished in any manner, however, if the trend persists, law enforcement agencies will soon have no workable avenues by which to extract digital evidence from modern smartphones in investigations of serious and organized crime.

§ 2.6.13 IoT-Specific Problems

Smart homes, connected devices, wearable gadgets, and even human-implanted chips and remotely manageable insulin pumps have been penetrating into society for over a decade, posing a new set of fuzzy challenges for digital investigators (Oriwoh et al., 2013). Given the unfolding series of privacy scandals in recent years, such as the unwarranted disclosure of sensitive data from Internet of Things (IoT) devices to law enforcement agencies (Crist, 2022), one may perceive connected objects as free rocket fuel to propel criminal investigations. Especially given the petabytes of sensitive data that IoT objects daily process and store, one may have an erroneous perception that the IoT is a contemporary El Dorado for cyber units of law enforcement agencies. Alas, although connected objects do increasingly store and process digital

evidence indispensable to clear serious crimes, the ugly reality of IoT investigations is quite the opposite of an untroubled and tranquil data-collection expedition.

The modern-day realm of IoT devices and connected objects progressively morphs into a multidimensional Internet-of-Anything (IoA), with numerous vertical sectors and horizontal niches, consolidating IoT ecosystems of previously unimaginable size and scale, ranging from nationwide networks of interoperated smart grids to primitive electronic gadgets sold online for a few dollars (MacDermott et al., 2018). Pertinent examples include a megapolis-wide traffic light management system, designed to receive data from thousands of smart captors and Closed-Circuit Television (CCTV) cameras, which are eventually aimed to coordinate and fluidify automobile traffic in the city; an automated air-conditioning system in a skyscraper, which intelligently regulates office temperature depending on the number of people in each room on each floor; a life-saving emergency break functionality in autonomous cars, equipped with intelligent road sensors; a smart boiler connected to an external thermostat to automatically adjust house heating; a surveillance drone, carrying stealthy video cameras and capable of automatically alerting police the in case of detected danger; a wearable bracelet or smartwatches designed to immediately notify the owner's relatives or doctor if the owner's pulse suddenly falls into a dangerous range; and low-cost toys with built-in cameras and microphones, connectable to a home wireless network, so parents can monitor their infants (Janarthanan et al., 2021). Remarkably, the contemporary IoT industry is characterized by its relative immaturity, lack of regulations for product safety and security, comparatively low entry barriers for new manufacturers, and the mushrooming number of device manufacturers around the globe. Somewhat paradoxically, the foregoing issues have two diametrically opposed outcomes for IoT investigations conducted by law enforcement agencies, which are discussed below.

On one side, many IoT devices are vulnerable and insecure by design, raising serious concerns over data protection and privacy (Neshenko et al., 2019). Even some high-end, branded, and expensive IoT devices may have unprotected administrative interfaces, permitting to gain full control over the device without entering a password. Worst, some devices do not even provide the basic functionality to set up or change the default password. Other connected objects store all data without any encryption on the device or, conversely, send all the data to a central repository in an unprotected cloud storage or Firebase database, from which it can be accessed by anyone without any authentication. As frequently, IoT devices have Internet-connected interfaces that can be easily compromised by well-known and simple attacks, allowing cybercriminals to take full control of the vulnerable device (Servida & Casey, 2018). This is not to mention comparatively advanced attack scenarios, for instance, when an IoT device authenticates into a remote database, storing sensitive data from all other users, and prone to privilege escalation or improper access control attacks, eventually enabling a remote attacker to extract all records from the database. Notably, in dealing with the cloud-based backend of an IoT device, one simple misconfiguration (e.g., the hardcoded access key of a privileged user) may allow a remote attacker to pivot into other cloud resources and eventually compromise the entire cloud environment and the interconnected systems of the manufacturer (Stoyanova et al., 2020). The above scenarios dispel the misconception about the absolute ease of digital investigations implicating IoT devices. The next section brings even more chilling reality into the context.

IoT devices are frequently equipped with heterogenous, customized, or even tailor-made hardware, firmware, and software, making evidence acquisition a highly unpredictable and non-standardizable process, as almost every investigation brings something new to the process. Even the most popular gadgets, massively commercialized by tech giants such as Amazon, may differ

substantially from one device version to another. When sending the data outside of the device, most connected objects rely on an entangled stack of network communication protocols, spanning from obsolete to ultramodern, as well as proprietary ones (Yaqoob et al., 2019). Eventually, the entire multistep process of IoT digital forensics, from evidence acquisition to reporting, becomes vendor-specific, firmware-specific, and even device-specific, boosting both the costs and time required to properly extract digital evidence, even without mention of the requisite technical skillsets of police detectives. In sum, an insecure IoT device, which can be easily hacked by cybercriminals, is not necessarily synonymic to a device that can be easily investigated by police to properly extract electronic evidence that would be adducible in court. Moreover, numerous vulnerabilities or design flaws can often indicate the overall poor quality of an IoT device, eventually making the IoT forensics process unpredictable and opening the door to claims that all and any electronic evidence obtained from the device is unreliable.

In continuation, Stoyanova et al. (2020) comprehensively systematized the modern-day problems faced by digital investigators in relation to contemporary IoT forensics. One of the prevailing obstacles is the identification of the sought evidence, as the data may be stored on the IoT device built-in storage, on the device's middleware (e.g., a smartphone connected to the IoT device via an app to manage it), or even remotely in a public cloud. Sometimes, all these variants co-occur, spraying digital evidence and forensic artifacts into a radius of multiple countries or even continents. Another major challenge relates to evidence acquisition: IoT manufacturers may use proprietary storage formats, compression methods, or encoding of data on the device. To retrieve and read such data, police investigators may first need to reverse engineer the peculiar format's structure and then create a custom script to convert raw data into a readable file. Therefore, even when programmatically doable, eventual success of investigation is never

guaranteed: hardware design and small data storage capacities of IoT devices can usually store just a tiny volume of data on the device, meaning that historical data is progressively overwritten by the more recent data. Further, if the data is accumulated in a cloud environment, the cloud-specific nuisances, reviewed above, come into the game. Making the situation even more hopeless and unpromising, some large IoT device manufacturers have started to inch towards default data encryption and the concomitant parade of forensic troubles discussed at the beginning of this chapter. Finally, evidence preservation and authentication are grueling tasks for IoT forensics: depending on the specific jurisdictional requirements and rules regarding the electronic evidence, it may be flatly unfeasible to seize the data in a forensically sound manner, or without damaging the device due to software or hardware particularities. For instance, manual data acquisition is likely to be impossible without altering the data, whilst in other scenarios the extracted files may have unreliable or even random timestamps, eventually making it impossible to prove when a specific event really took place (Stoyanova et al., 2020).

Legally, based on the jurisdictional and procedural nuances discussed above, the actual geographical scope and perimeter of an IoT investigation are pervasively murky and unpredictable, despite having physical access to the device. As explained above, the data sought may be located outside of the device in many places at once, crafting convoluted dilemmas for judges and prosecutors about the scope of the warrant required to seize the electronic evidence, let alone the problems of jurisdiction over foreign evidence, as discussed in a previous section. Notwithstanding the mounting number of proposals to create a forensically sound investigatory framework for IoT devices, the legal and procedural sides of the process remain nascent and undeveloped across most jurisdictions and cannot be leveraged with certainty in courts (Bouchaud et al., 2021; Janarthanan et al., 2021; Lutta et al., 2021). In sum, the foregoing

technical intricacies and legal and procedural pitfalls of IoT investigations may transform them into a cost-prohibitive and futile exercise for law enforcement agencies.

§ 2.7 Examples of Legislative Responses

In response to the foregoing array of technical, operational, and legal challenges to the seizure of electronic evidence and crime investigations, legislators around are globe are progressively implementing new statutory laws and sector-specific rules purported to overcome, or at least to alleviate, some of those challenges. Courts are also actively contributing to the process by developing case law and setting new precedents in national jurisprudence. Below, the researcher will briefly review the main legislative trends, which have a varying degree of success and practicality, as well as their implications.

§ 2.7.1 Mandatory Backdooring

Hypothetically, the most straightforward countermeasure to the global proliferation of strong encryption would be to obligate device and software manufacturers to implement a form of backdoor, or hidden functionality, into their technologies that would be accessible to national law enforcement agencies to gain access to unencrypted data and communications. Far from being novel, this idea emerged in the mid-1990s in the United States (Walden, 2018). After protracted and heated debates with the technology industry on the mandatory backdooring of encryption technologies—the decade-long feud known as “Crypto Wars” —the U.S. government finally abandoned this initiative, facing unprecedented resistance and well-reasoned opposition from major industry players, scholars, and experts (Koops & Kosta, 2018).

Rivest (1998), the co-inventor of Rivest–Shamir–Adleman (RSA) encryption and a venerated American cryptographer, persuasively summarized the deficiencies of mandatory governmental access to hidden decryption mechanisms. Firstly, he remarked that terrorists,

foreign spies, and dangerous criminals may quite easily circumvent such regulation by implementing their own encryption protocols, algorithms, or software—even if flatly prohibited by law—eventually leaving the government with a sole and questionable capacity to spy on its own law-abiding citizens. Secondly, whilst conceding that strong encryption is a dual-use technology, he argued that the benefits of its legitimate usage, namely the prevention of data theft from corporations and governmental agencies by malicious insiders or foreign hackers, significantly surpasses the negative effects of encryption misuse by nefarious criminals. Thirdly, he indicated that the proposed solutions of key-recovery and key-escrow, which would allow the government to decrypt any regulated encryption within the country, would be exorbitantly expensive to implement and maintain, and—perhaps most importantly—would inevitably become an irresistible magnet for skilled cybercriminals. He further stressed that if the governmental decryption infrastructure is compromised, this would open the floodgates of a massive theft of trade secrets, facilitate the interception of top-secret state communications by foreign adversaries, and consequently provide threat actors with unrestricted access to the confidential data of every American company, governmental agency, and resident. He cogently concluded that, from an economic viewpoint, weakening encryption technologies with a mandatory backdooring would inevitably undermine the global competitiveness of U.S. companies and annihilate its then-undisputed status as a technology pioneer (Rivest, 1998). Additionally, among other arguments against encryption backdooring asserted by the industry, it was contended that some federal governmental agencies could potentially abuse their unbridled decrypting power, for instance, by massively leveraging it in banal criminal investigations, when such intrusive measures of investigation would be disproportionate, inadequate, and costly for the state, without even mentioning privacy concerns.

In the more recent revivification of debates over the mandatory backdooring of encryption technologies to make them decipherable by government, Schneier (2015), one of the most venerated cryptographers of the modernity, expressed his frank skepticism over the backdooring approach. He shared statistics from George Washington University that, back in 1999, identified over 500 cryptographic companies in more than 70 countries around the globe, offering strong encryption technologies whilst being beyond the legislative reach of the U.S. Congress. Schneier warned that even if a mandatory backdooring legislation project one day passed into a federal law, sophisticated wrongdoers would simply shift to foreign, unregulated, and unregulatable encryption technologies, leaving U.S. federal agencies in darkness again, though with a controversial capacity to read the daily communications of U.S. citizens (Schneier, 2015). One year later, he convincingly reiterated his anti-backdoor position by enumerating the indisputable benefits of encryption for society and the inescapable risks of backdoor misuse by sophisticated and state-backed threat actors in cyberspace (Schneier, 2016).

A report produced by the United Nation's Office of the High Commissioner for Human Rights (OHCHR) in 2015 went even further, proclaiming that encryption is essential for human rights and for freedom of opinion and expression and, thus, that it should be safeguarded by all reasonable means, including outlawing backdooring (Peterson, 2015). In 2018, a consonant anti-backdoor position was enunciated by the Article 29 Working Party—replaced by the EU EDPB in May 2018—in its telling statement on encryption and its derived impact on the secure processing of personal data within the EU (Working Party, 2018). The statement emphasized the ultimate importance of strong encryption required to safeguard sensitive data, namely personal data as, for instance, as expressly required by the EU GDPR. Likewise, the statement pointed out that a 100% secure implementation of backdooring capabilities, which would be invulnerable to

hacker attacks and resilient to internal misuse, would be technically unachievable and utopic. The Working Party elegantly summarized the inefficiency, non-effectiveness, and eventual harm of mandatory backdooring:

> Moreover, imposing backdoors and master keys on law abiding citizens and organisations would not be an effective measure against criminals since they would continue to use or adapt the strongest state of the art encryption to protect their data, keeping them safe from law enforcement access. As a result, backdoors and master keys would only harm the honest citizen by making their data vulnerable. (Working Party, 2018, p. 2)

Remarkably, to proactively tackle the foregoing concerns, the Netherlands pioneered a protection of strong encryption at the national level. In 2016, the Dutch government made it crystal clear that backdooring would not be a viable option to combat serious crime and terrorism sustainably (Kovacs, 2016; Veen & Boeke, 2020). In addition, scholars concurred that compulsory backdooring will likely have a palpable impact solely on laypeople, who are already intensively monitored by lawful means of telecommunications and internet surveillance around the clock, whilst criminal kingpins and their chief acolytes will aptly combine multilayered encryption mechanisms, making them invulnerable to state's backdoors (Murphy, 2020). Developing the argument on the pitfalls and hazards of backdoors, as well as hidden vulnerabilities that would allow law enforcement to remotely take control of electronic devices, Farlow and Edwards (2022) highlighted that "there is no guarantee that this technological weakness cannot be discovered by hackers, advanced persistent threats (APTs) or misused by those with knowledge of the weakness" (p. 10).

Marking a bewildering shift in a diametrically opposed direction, the European Commission (EC) recently proposed new legislation formally designed to protect children from

sexual violence by, inter alia, requiring service providers to be able to monitor all digital communications of their clients to detect child pornography (Mullin, 2022). Given that quite similar objectives can be attained with considerably more privacy-friendly technology, such as hash-matching of transferred files to spot known illicit content (Apple, 2021), this proposal predictably provoked an avalanche of critique from privacy advocates and the tech industry. If one day accepted, this legislation may factually oblige service providers to spy on their users, under the unquestionably laudable pretext of child protection, but to the grave detriment of legitimate users' privacy and security. Eventually, one may hypothesize that if one day users' communications become accessible to service providers, law enforcement agencies will certainly find their way to seize such an unmissable opportunity for all other types of investigations, going far beyond sexual exploitation of children. Somewhat foreseeably, the EC's proposal was scrutinized and then widely criticized in a joint statement made by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) for, among other things, endangering people's fundamental human rights (EDPB & EDPS, 2022). The unambiguous statements of the EU privacy watchdogs manifestly communicate that the proposed EC legislation is unlikely to be accepted in its current form.

Despite the mounting number of calls and creative regulatory proposals in favor of legislation that would render encrypted data decryptable with, or even without, a court order (Murphy, 2020), the future of such legislation is largely uncertain. Any legislation aimed to weaken or suppress encryption will highly likely be at odds with the individual privacy and other protectable human rights, and hence be prone to judicial invalidation, for instance, after being declared unconstitutional in those jurisdictions where courts have the authority to strike down laws that violate constitutional rights or rights protected by international treaties (Koops &

Kosta, 2018). Therefore, law enforcement agencies shall not count on mandatory backdooring to simplify their digital investigations of serious and organized crime.

§ 2.7.2 Assistance by Service Providers

Another approach to defeat encryption contemplates a unilateral shift of the burden to the shoulders of privacy-friendly service providers. For instance, in the United Kingdom, under provision of the Investigatory Powers Act (IPA) of 2016, communications service providers are required to provide law enforcement agencies with reasonable assistance to decrypt their customers' communications when the encryption is implemented, controlled, or operated by the provider and when it is technically possible to do so (Walden, 2018). Whilst this type of collaboration is much less intrusive and risky than is the backdooring previously discussed, many provisions of the IPA triggered vigorous debates about the allegedly overbroad power granted to the U.K. government under the Act, factually implementing disguised backdoors without labeling them as such (Lomas, 2016). Remarkably, a provider's deliberate failure to cooperate in the United Kingdom is a criminally punishable offense (Walden, 2018; Dizon & Upson, 2021), making submissive cooperation the least risky choice. The implications of E2E encryption are discussed below.

Similar, albeit less strict, provisions are also available under U.S. law, requiring service providers to intervene pursuant to a court order and disable encryption implemented by the provider, as codified in the Communications Assistance for Law Enforcement Act (CALEA) of 1994 (47 U.S. Code § 1001 - 1010):

> A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, *unless* [emphasis added] the encryption was provided by the carrier and the

carrier possesses the information necessary to decrypt the communication. (47 U.S. Code § 1002 (b) (3))

The regulatory scope of the now-obsolete CALEA applies solely for telecommunication service providers, excluding device manufacturers (e.g., Apple) from the scope of compelled assistance (Hill-Smith, 2019). Several proposals were recently made to expand the current scope of CALEA, namely the proposed Compliance with Court Orders Act (CCOA) of 2016 draft legislation (Poplin, 2016). However, at the time of writing, all the proposals faced a crushing fiasco after the fierce resistance and snowballing critique from industry and privacy advocates (Hennessey, 2016). In parallel, in creative attempts to fill out the legislative gap, U.S. law enforcement agencies have attempted to leverage the All Writs Act of 1789 (28 U.S. Code § 1651) as a sword in litigation, with varying degree of success. For example, in the infamous San Bernardino mass-murder case, the FBI attempted to use the Act to compel Apple to unlock the shooter's iPhone, eventually obtaining the order from the magistrate judge. Apple fulminated and announced its intention to vigorously appeal the path-breaking order, stating that it could set a dangerous precedent. In the meanwhile, an external company hired by the FBI managed to successfully unlock the device. Therefore, to the firm regret of both opponents and proponents of the ruling, the potentially landmark appeal never took place. The possible outcomes of the appeal are conjecturally speculative, and no prevailing opinion exists among legal scholars concerning the appeal's possible outcome (Hill-Smith, 2019).

Importantly, with the ubiquitous proliferation of the end-to-end encryption (E2EE), as underlined by Veen and Boeke (2020), collaboration by service providers becomes technically impossible and unfeasible in most cases. Theoretically, his may exonerate service providers truly unable to help authorities with decryption, when their users enable E2EE, from being sanctioned

for noncompliance with a court order or enacted law. Although some scholars suggest that under the provisions of the U.K. IPA, service providers are expected, and may even be forced, to remove or temporarily disable E2EE and provide the government with access to an interceptable channel of communications (Murphy, 2020). Whilst such a measure is likely to be affirmed in U.K. courts, its eventual deployment will probably remain modest due to the inescapable public outrage in the case of its mass deployment.

On the other side of Atlantic, the U.S. Department of Justice (DoJ) castigated E2EE encryption for making crime prevention undoable, disarming law enforcement agencies, and preventing service providers from enforcing their own terms of service against users who, for instance, may freely share child-abuse materials or promulgate hate speech with impunity (Department of Justice, 2020). In its alerting statement, the DoJ called for enhanced collaboration with service providers, aimed to create an environment that would allow the interception and policing of illegal content by circumventing E2EE. It is, however, highly unlikely that one can expect service providers to voluntarily weaken or disable their E2EE mechanisms amid soaring pro-privacy marketing campaigns and competition for privacy-savvy customers. The same year, being more pragmatic about the industry's reluctance to collaborate, Europol launched a central platform to offer decryption services to EU law enforcement agencies (Europol, 2020). Whilst this is a laudable and smart initiative, it is unlikely that the platform will help break E2EE or other variations of strong encryption, instead offering assistance with cases only when circumvention is technically possible and economically practical, for instance, through the exploitation of known implementational weaknesses or software vulnerabilities.

The mandatory collaboration of service providers with law enforcement agencies is a rapidly evolving area of law susceptible to uncertainty and to intermittent grey areas. Obviously,

no vendors are willing to invest their own resources to support law enforcement, as doing so would cause them to face reputational risks and possible loss of their market share. In the past, some countries have attempted to enforce a mandatory collaboration regime for service providers, backed with harsh penalties for providers unwilling to comply. For example, France suggested imposing €1 million fine on Apple per each unlocked iPhone (Tung, 2016). However, such controversial, one-sided laws are anticipated to face mounting opposition from public and tech industry, making the future of such legislation unforeseeable and unstable, to put it mildly. In sum, at the time of writing, law enforcement agencies have to count only on themselves in the digital battle against serious and organized crime.

§ 2.7.3 Compelled Password Disclosure

Compelled disclosure of smartphone passcodes, data encryption keys, or computer passwords may be a potent arm in the law enforcement's arsenal against the overshadowing encryption discussed in the previous sections. This fascinating idea seems to be attractively simple: coerce suspects to disclose keys from their digital safes to police investigators under penalty of severe criminal punishment (Walden, 2018). The existing legislation on compelled disclosure is, however, heterogeneously polarized from one jurisdiction to another, being subject to countless procedural nuances and subtleties. It is thus a thorny way forward for police officers wishing to unlock incriminating electronic evidence by reasonable use of coercion.

Arguably, the United Kingdom has one of the most powerful sets of legal instruments for extracting secrets from human minds. The U.K. Regulation of Investigatory Powers Act (RIPA) of 2000 equips law enforcement agencies with a right to demand password disclosure under Section 49 when it is necessary, among other things, to prevent or detect crime. Under Section 53 of RIPA, a refusal to comply is punishable by imprisonment of up to two years; in cases

implicating national security or child indecency—up to five years. However, the prosecution must demonstrate that the suspect actually possesses (i.e., knows) the password (or other secret) and that the password is reasonably required for the investigation of criminal offense and will likely bring relevant evidence that cannot be obtained by less intrusive means. So far, several attempts to argue that forced disclosure violated suspect's right against self-incrimination have been unsuccessful in the U.K. courts (Keenan, 2019).

In continental Europe, most countries cannot compel a suspect to disclose passwords in criminal investigations with some notable exceptions such as Belgium, where coerced disclosure was found lawful and constitutional (Kargopoulos, 2021). A similar regime is enacted in France, whilst Norway has pioneered coerced device unlocking through the use of biometric authentication—though not without simmering indignation from privacy advocates and civil rights activists, who argue that compelled unlocking is a flagrant violation of the right to a fair trial and the right against self-incrimination (Fukami et al., 2021). The ongoing debates, the innate legal ambiguity, and the ensuing litigation over the legality of compelled disclosure may partially stem from the EU Directive 2016/343 of 9 March 2016. The Directive somewhat provocatively states that:

> The exercise of the right not to incriminate oneself should not prevent the competent authorities from gathering evidence which may be lawfully obtained from the suspect or accused person through the use of legal powers of compulsion and which has an existence independent of the will of the suspect or accused person, such as material acquired pursuant to a warrant, material in respect of which there is a legal obligation of retention and production upon request, breath, blood or urine samples and bodily tissue for the purpose of DNA testing. (EU Directive 2016/343, Section 29)

In creative interpretations of the directive text, some European jurisdictions consider passwords to exist independently of the suspect's will, akin to fingerprints or DNA samples, whilst others have a diametrically opposed and pro-privacy worldview. "Black Swan" events such as Brexit, add another cascade of legal controversies, for example, whether EU law incorporated into U.K. law will be gradually amended or repealed (Lowe, 2021). Thus, in the post-Brexit European legal landscape, the compelled password disclosure will likely remain persistently volatile and largely uncertain, let alone in other countries where the legislation is nascent or simply absent.

In the United States, the situation is even more intricate and unsettled. Edmonson (2021) indicates that compelled disclosure may be in irreconcilable conflict with the Fifth Amendment of the U.S. Constitution, which protects suspects against self-incrimination. As demonstrated by case law, the Fifth Amendment may be, in its turn, negated by the decades-old Foregone Exception, wherein the existence of compelled information is already known to authorities. The exception originally addressed the compelled disclosure of paper documents and is, thus, somewhat unfit for modern-day passwords. State courts from different U.S. states, as well as federal courts from different circuits, apply the Exception in opposed and conflicting manners, creating a pressing climate of judicial unpredictability that will persist until the Supreme Court finally rules on the Exception's applicability for the numeric world (Edmonson, 2021; Kerr O. S., 2021). Sadly, in light of the recent refusal of the Supreme Court to hear an appeal involving the crux of the exception, there is a little hope for clarity in the foreseeable future (Merken, 2021).

In conclusion, from a purely practical viewpoint, compelled password disclosure may be an efficient instrument against first-time offenders or when dealing with trivial crimes involving

digital secrets. Inversely, seasoned members of criminal conglomerates will likely be undaunted by a light prison sentence for refusing to cooperate, as the alternative is to regret about their imprudent decision to collaborate with police behind the bars for the rest of their lives. Illustrating this point, there are known cases of suspected murderers escaping a conviction for murder but being eventually imprisoned for their refusal to hand their passwords to authorities (Cuthbertson, 2018). Worse, in other jurisdictions, for example in Switzerland, even such a utilitarianly modest outcome is unimaginable, as no legislation exists to compel password disclosure. Therefore, law enforcement agents are again parachuted into the cyber battlefield with heavily armored troops of serious criminals, having no tenable legislative reinforcement or backup.

§ 2.7.4 Criminalization of Encryption Misuse

This legislative instrument is, arguably, the most conventional, reasonable, and usable under some circumstances. The encryption criminalization approach addresses the bad-faith use of encryption to further a criminal conduct or to deliberately hinder investigations by law enforcement agencies. Such tech-driven misbehavior can be criminalized as a separate criminal offense under a national penal code, increasing the offense's degree and, thus, its minimum punishment threshold. It may also be considered an aggravating circumstance during sentencing after the guilty verdict. The three aforementioned approaches are implemented into the criminal law of the U.S. state of Virginia, France, and the United Kingdom, respectively (Walden, 2018).

Being privacy-neutral and unintrusive, compared to other methods discussed above, the criminalization of encryption misuse may serve as a sound deterrent for offenders and could prevent crimes under the deterrence theory discussed in Chapter 1. Firstly, when faced with a dilemma including a more severe penalty and a lesser one, a would-be offender may eventually

abandon the idea of committing crime. Secondly, as offending without encryption increases the chances of arrest, indictment, and eventual conviction in a court of law, this legislative measure may dissuade would-be infringers from breaking the law. That being said, this non-contentious, privacy-friendly, and socially reasonable approach may have a positive, albeit insignificant, impact on the overall reduction of crime.

Nonetheless, similar to the approach of compelled password disclosure under penalty of imprisonment analyzed in the previous section, the impact of the criminalization of encryption misuse will likely primarily affect first-time or juvenile offenders. Recidivists and battle-seasoned hitmen from organized gangs will unlikely be intimidated by an extra year or two in prison when facing a lifetime sentence in the case of their arrest and successful prosecution for more serious crimes. Therefore, this attractive and privacy-neutral approach will provide law enforcement agencies with little-to-no recourse in the intensifying fight against serious and organized crime that exploits encryption and other technical instruments to shield their villainy.

§ 2.8 Lawful Hacking as a Better Alternative

For some time, lawmakers from different countries have been considering lawful hacking as an expedient alternative to, or reinforcement of, the existing legislative mechanisms discussed in the previous section. Bercovitz (2021) indicated that “commentators have long called for statutory regulation of NIT [Network Investigative Techniques i.e., lawful hacking] searches” (p. 1281) to bring certainty, transparency, and predictability to digital investigations by law enforcement agencies, while setting tenable standards of privacy protection in parallel. Likewise, industry experts have been consonantly advocating the legalization of lawful hacking for over a decade already. For instance, Kolb (2007) proposed the interception of VoIP communications by means of lawful hacking back in 2007 through the backdooring of a suspect’s device and

recording of otherwise non-interceptable Skype communications. At the time of writing, the overall state of lawful hacking legislation is still quite nascent and heterogeneous from one jurisdiction to another. Although, most countries have enacted some rudimentary form of lawful hacking legislation (Sommer, 2022) by enacting a specific statutory law, by acquiescing to judicial decisions that ingeniously extrapolate long-existing legal statutes or judge-made doctrines over offensive operations in cyberspace, or by promulgating administrative rules and regulations when administrative rulemaking in relation to lawful hacking is permitted. Eventually, this patchwork of lawful hacking legislation incentivized law enforcement agencies, mostly from countries where investigations by lawful hacking is unwelcomed in courts, to explore "jurisdictional forum shopping" opportunities, defined by Davies (2020) as "purposefully collaborating with an overseas LEA [Law Enforcement Agency] as a way of circumventing national rules relating to the conduct of an investigation" (p. 413). While being a licit practice, such ingenuity is unlikely to please opponents of lawful hacking legalization.

It has been argued that hacking is excessively intrusive or even violent by nature and thus may be inappropriate for law enforcement agencies, from both an ethical and a moral viewpoint (Bellovin, 2021). The same, however, can be said about on-duty police officers that use their weapon to neutralize armed robbers or stop hijacked cars in hot pursuit. Nowadays, modern-day gangsters skillfully exploit technological progress to further or conceal their nefarious crimes. Therefore, a symmetrically modern response is necessary to adequately protect the wellbeing of society, its most vulnerable members, and the rule of law. Accordingly, the emerging phenomenon of lawful hacking seems to be inseparable from the future of justice and law in society, being an inalienable component of its natural evolution.

From a purely technical, pragmatic, and results-oriented viewpoint, lawful hacking provides undisputable advantages to law enforcement agencies for the efficient and effective digital investigations of serious and organized crime. Firstly, qualified cybersecurity experts can subvert virtually any type of encryption without actually decoding the encrypted data: sooner or later, offenders will access the data in question, and at this moment, the decrypted data will be stealthily seized and swiftly transferred into the possession of prosecution. The same applies for instant communications between wrongdoers: a carefully implanted backdoor may silently intercept and record any live communications and capture text messages, voice, or video communications in real time before they are encrypted or deleted. Eventually, the gamut of data volatility and unavailability problems, discussed at the beginning of this chapter, will vanish or at least become technically solvable. Secondly, by deploying lawful hacking, competent law enforcement agencies are the only parties who actually enjoy full control over the digital investigation process, without a fear of premature disclosure or automatic notification by a third-party service provider—also discussed above—which may eventually ruin many years of painstaking and grueling investigation. Thirdly, when lawful hacking is properly executed by experienced cyber professionals, the entire process of digital evidence identification and extraction will likely become faster and less costly compared to other methods, eventually saving taxpayers' money. Fourthly, if lawful hacking finally becomes holistically regulated and expressly authorized by law, the mounting number of legal problems, namely the inadmissibility of digital evidence in court, will swiftly vaporize for everyone's benefit. Fifthly, the proactive nature of lawful hacking may prevent serious crimes rather than modestly assist in the post-mortem investigation of a mass murder, child rape or abduction. Finally, but importantly, technology vendors and service providers will be exempt from introducing backdoors or hidden

vulnerabilities into their systems or services, which would unavoidably jeopardize their security and integrity akin to a ticking timebomb.

As mentioned in the previous chapter, the first mentions of governmental agencies trying to leverage computer hacking for crime investigations are almost three-decade old. In the United States, law enforcement agencies were reportedly breaking into remote computers and installing the first generation of backdoors back in 2001 (Lynch, 2011). In Europe, the commencement of a systematic approach to hacking by authorities can be traced back to early 2007, when the German government indirectly unveiled its ambitious plans to develop a "remote forensic software"—a Trojan horse for presumably large-scale offensive operations in the cyberspace (Leyden, 2007). In parallel, the U.K. police reportedly conduced at least 194 "hacking operations" from 2007 to 2008; it is, however, unclear whether at this time they already possessed proprietary backdooring technology (Morris, 2009). At almost the same time, in November 2008, the Council of the European Union presented a then-groundbreaking report entitled "Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime," suggesting that "member states should introduce clandestine remote searches of computers as a standard investigation method to combat cybercrime" (Abel, 2010, p. 99). Whilst Abel (2010) expressed judicious reservations and concerns over lawful hacking by police, citing, inter alia, the eventual inadmissibility of such digital evidence in court proceedings, the possible violations of human rights and privacy laws as a result of cyber investigations, and the convoluted jurisdictional problems in relation to the territoriality of seized digital evidence, he pointed out that the report "has sent a clear message that [lawful hacking] will become a standard investigation method in the future" (p. 107) and that lawful hacking has "the potential of increasing the efficiency of investigative actions" (p. 107). Interestingly, back in 2012, the U.S.

Drug Enforcement Administration (DEA), possibly invigorated by the above-mentioned report, invested at least $927,000 into the acquisition of cyberwarfare for remote investigations of international drug trafficking (Brown, 2020).

With his pioneering publication on lawful hacking, Abel (2010) set the scene for future scholarly research. In a subsequent publication covering numerous aspects of lawful hacking, which later became the milestone work on the subject matter, Bellovin et al. (2014) elaborated and analyzed possible operational and legal impediments to streamlined lawful hacking as a better alternative to the mandatory backdooring or weakening of encryption. In the thought-provoking publication, the prominent legal scholars comprehensively examined several multifaceted and multidisciplinary topics, including the impact of lawful hacking on innovation and vulnerability patching, the technical readiness of law enforcement agencies to competently conduct hacking operations in a scalable and cost-efficient manner, the ethical and legal risks of buying zero-day vulnerabilities and exploits on the grey market, and the perils of the misappropriation of cyberwarfare developed by police. In their conclusion, the scholars warned of the wide spectrum of risks related to carelessly conducted lawful hacking operations and suggested several practical steps to reduce those risks and even reverse the negative impact of lawful hacking to eventually build a more secure Internet. Likewise, while highlighting that negligently performed lawful hacking is prone to a plethora of hazardous drawbacks, they stated that lawful hacking "is preferable for conducting wiretaps against targets when compared to other possible methods of wiretapping, like deliberately building vulnerabilities into the network or device" (p. 64). Three years later, Swire (2017) reiterated this sound position on lawful hacking, stating that as long as there is no clear-cut legislation on lawful hacking, the government has strong incentives to pursue doubtful avenues of mandatory backdooring and

other contentious techniques to seize digital evidence in criminal investigations, opening the door to various abuses or collateral effects of investigations conducted in cyberspace. Later, Fidler (2020) likewise suggested that without a crystal-clear regulation and appropriate judicial oversight over lawful hacking operations, state law enforcement agencies will likely deploy overbroad or otherwise improper techniques to gather digital evidence, to everyone's detriment.

A collateral effect of the legal vacuum in relation to lawful hacking, being undesirable both for society and criminal justice system, does exist in jurisdictions where the defendant has a right to demand the disclosure of the operationalized investigatory techniques, including the source code of spyware and the hacking tools or exploits utilized by cyber detectives. Those rights created a phenomenon of "grey mailing," where defendants demand the full disclosure of cyber investigation tools and techniques in court (Bell, 2018). For instance, in the United States, cases are known where the prosecution preferred to drop all charges and dismiss the case instead of disclosing its methods of cyber operations, protecting its intellectual property from being scrutinized by third-party experts or even from being publicly disclosed (Garcha, 2018; Fidler, 2020). Resultingly, in the legal emptiness, criminals will attempt to abuse the subtle nuances of the judicial process and procedure to waste judicial resources and to disincentivize prosecution from bringing charges corroborated by electronic evidence, eventually fostering the proliferation of crime amid the impunity of criminals and feebleness of law enforcement.

Recent scholarly research continued and expanded the legendary works of Abel, Swire, and Bellovin. For example, Liguori (2019) proposed specific prerequisites and limitations for lawful hacking operations, precautions for the acquisition and development of cyberwarfare, and possible answers to the accumulating jurisdictional issues in relation to the digital evidence

seized from abroad. In his work, he affirmed the rationale and conclusions in favor of lawful hacking from the previously published works supporting cyber operations by police:

> Lawful hacking seems to be a viable alternative to the restriction of encryption or the mandatory exceptional access: Instead of requesting technology companies to sabotage their own security systems and knowingly compromise the security and privacy of their users, this alternative focus on observing and exploiting preexisting (and often unintended) security holes. (Liguori, 2019, p. 329)

In a more recent publication, Bellovin (2021) briefly reminded readers about the magnifying risks of lawful hacking, but unambiguously called for its final legalization through the implementation of a privacy-friendly legislation that would expressly authorize offensive cyber operations to investigate and prosecute serious crime. The urgent need for transparent regulation of lawful hacking, which would draw a straight and bold line separating the permitted cyber operations from the illicit ones, is also necessary to provide a safe harbor for cybersecurity vendors, such that they can assist law enforcement agencies without the grave risk of being sued or even criminally prosecuted for transcending the border or permitted cyber operations (Rozenshtein, 2019). Departing from the Bellovin's position, Hewson and Harrison (2021) enumerated the possible pitfalls of lawful hacking, but likewise acknowledged that, if properly regulated and diligently performed, lawful hacking can be a much better alternative to "introducing vulnerabilities into strongly encrypted systems," that may eventually lead to "seriously endangering members of vulnerable or minority groups, and may compromise official communications" (Hewson & Harrison, 2021, p. 6).

The foregoing posture of legal scholars, inclined towards the legalization of lawful hacking, is naturally shared by the Western law enforcement community. In 2016, the Europol

and the European Union Agency for Cybersecurity (ENISA) released a joint statement justifying the pressing need to implement lawful hacking for the investigation of serious crime (Europol & ENISA, 2016). The report cogently summarized the technical difficulties and insurmountable barriers faced by law enforcement agencies when dealing with search and seizure of digital evidence, whilst emphasizing that lawful hacking may be deployed only when proportional to the gravity of the investigated offense and when less intrusive means are unavailable. The report also judicially explained the advantages of lawful hacking over backdooring:

> Breaking into a digital service might be considered as proportional with respect to an individual suspect, but breaking the cryptographic mechanisms might cause collateral damage. The focus should be on getting access to the communication or information; not on breaking the protection mechanism. The good news is that the Information needs to be unencrypted at some point to be useful to the criminals. This creates opportunities for alternatives such as undercover operations, infiltration into criminal groups, and getting access to the communication devices beyond the point of encryption, for instance by means of live forensics on seized devices. (Europol & ENISA, 2016, p. 1)

Reflecting the equilibrated and well-balanced position of the two major pan-European law enforcement agencies, a report from the EastWest Institute proposed a choice of two distinct regulatory regimes, designed to tackle the misuse of encryption by organized crime. The first regime suggests the legalization of carefully regulated lawful hacking, offering a large umbrella for comprehensive privacy protection in parallel. Whilst being written in prudent, privacy-oriented, and neutral language, the report brings extra clarity to the indisputable technical advantages of lawful hacking:

> Lawful hacking may exploit vulnerabilities in systems and devices, whether remote or local, or use social engineering to circumvent security protections. Law enforcement may deploy lawful hacking as a technique to gain access to a system to intercept communications, secure digital evidence or facilitate access to stored data or communications in plaintext. (EastWest Institute, 2018, p. 7)

The researcher believes that, whilst it may be subconsciously unwelcome by some, lawful hacking is poised to become an essential part of criminal justice, required to maintain a safe and sustainable society, preserve the rule of law, prevent serious crimes and violence in society, and ensure fair and certain punishment for offenders. Offering a validation to this belief, the European Union Agency for Law Enforcement Training (CEPOL) recently named lawful hacking among the key competences where EU law enforcement agencies need more training (CEPOL, 2021). In the next sections, designed to ensure a two-sided approach to the phenomenon of lawful hacking within the investigation of serious and organized crime, the intrinsic and extrinsic risks that may originate from lawful hacking are discussed, so they can be properly addressed by the framework in Chapter 4 of this dissertation.

§ 2.9 Risks of Lawful Hacking

Obviously, lawful hacking is not without its own drawbacks and pitfalls, particularly if conducted without a proper legal basis, due care, or necessary precautions. In 2019, in his though-provoking speech made before the Subcommittee on Crime and Terrorism of the Senate Judiciary Committee on data protection, William Carter, a Deputy Director at the Center for Strategic and International Studies (CSIS), covered the risks deriving from lawful hacking operations conducted by the government in response to the “Going Dark” phenomenon and from

the service providers' unwillingness to assist with the decryption of digital evidence required in investigations of serious crime:

> [Lawful hacking] is a fundamentally flawed approach that should be discouraged. Lawful hacking is by necessity opaque and unaccountable. If governments reveal their techniques and the vulnerabilities and exploits that they use to access data through lawful hacking, vendors will patch those vulnerabilities, rendering these tools ineffective. Lawful hacking is expensive and time consuming and requires significant technical resources and expertise, and law enforcement agencies around the world already struggle with significant resource constraints. Finally, and most importantly, promoting the use of lawful hacking by governments creates incentives that undermine global cybersecurity. It encourages more governments around to develop or acquire offensive cyber capabilities, fuels the growth of "grey market" firms like NSO group that are linked to ethically and legally questionable activities that threaten human rights and civil liberties, and discourages the disclosure of exploitable vulnerabilities to vendors so that they can be patched. (Carter, 2019, p. 11)

In response to the foregoing arguments, the researcher does acknowledge that a flawed regulation, imperfect execution, or lack of judicial oversight over cyber operations by law enforcement agencies within criminal investigations, or a combination thereof, may indeed have devastating consequences and cause irreparable damage to the fundamental values of society, the integrity of criminal justice system, and the rule of law. Regrettably, some fears, triggered by the impending legalization of hacking by authorities, tend to be exaggerated and can be presented in a one-sided context or confusing light. For instance, some otherwise well-written reports sound the alarm that governmental backdoors may be carelessly designed and eventually cause mass

damage to computers of innocent people. Other reports may present lawful hacking in an unnecessarily negative, pessimistic, or alarmist light, for example, emphasizing that backdoors provide "total control" over a device without sufficiently clarifying the context, details, and the eventual implications (Granick, 2017). To separate the wheat from the chaff, this research compiles below the most representative or serious risks that may arise from lawful hacking by law enforcement agencies within criminal investigations—if conducted in an inappropriate, careless, or unregulated manner. The possible solutions to prevent and mitigate those risks in a simple and cost-efficient manner are elaborated in Chapter 4, following a review of the existing lawful hacking legislation in Chapter 3 of this dissertation.

§ 2.9.1 Overbroad Scope

Some hacking techniques are intrinsically and inherently overbroad by their very nature or design and, thus, may accidentally compromise electronic devices unrelated to the investigation. For example, watering hole attacks, which have been deployed in the past by governmental investigators (Mayer, 2018), are purposely designed to compromise every user who visits a presumably trusted website by exploiting known or zero-day vulnerabilities in the victim's browser, or its components, to eventually backdoor the victim's device. Of note, watering hole attacks were predominately deployed by law enforcement agencies to compromise visitors of clearly illicit websites, such as web resources sharing child pornography, however, collateral victims, who may accidentally open such website cannot be totally excluded (Pfefferkorn, 2018). To minimize undesirable harm and collateral damage, watering hole attacks may, for instance, launch an exploit to compromise the website visitor only when certain meticulously predefined conditions are met, as with targeting visitors from a specific country or ISP, during a specific timeframe, or with a specific browser language, time zone, or device type.

Selective exploitation will certainly minimize the risks of infecting innocent passersby with a governmental backdoor, especially when the whereabouts or profiles of wrongdoers are known and can be used to narrow the list of possible targets. As an extra precaution, the exploit kit may be placed only on a single web page, preferably an old one or one unindexed by search engines. Once done, the link to the page can then be emailed or otherwise directly delivered to the suspect in a carefully prepared operation, excluding collateral victims. The foregoing precautions will eventually morph the watering hole attack into a spear-phishing attack combined with the usage of a trusted third-party website: with such laser-focused exploitation, the chances of collateral damage to innocent parties become infinitesimal. The preoccupations may, nonetheless, remain when the identity of the suspect is unknown, the suspect's device is shared by other users, or the malicious link is sent to a place accessible to the public (e.g., a group chat), eventually creating the undesirable risk of unintentionally compromising and backdooring innocent laypeople or accomplices from foreign jurisdictions and who thus may fall outside of the investigation (Brown, 2020).

A blurred or unclear horizontal or vertical scoping of the targeted infrastructure is a palpable predicament for offensive cyber operations within criminal investigations. The horizontal prong of the problem arises when the targeted device (e.g., a work, home, or college computer) is shared by several unwitting and innocent users who have no relation whatsoever to the probed crime (Brown, 2020). The vertical prong of the problem concerns excessive access to digital evidence belonging to the suspect but having no connection to the investigated offense. For instance, a suspected murderer, as a matter of law, indisputably deserves due protection of its tax declarations, divorce proceedings, privileged discussions with their lawyer, donations to political parties, health diagnoses, or financial records in circumstances where this information is

stored on the same device but has no connection to, or any probative value for, the investigation of the murder (Herpig, 2018). In practice, however, selective data exfiltration from a backdoored device is not always viable in cyber operations designed to stealthily and rapidly collect digital evidence and artifacts without being detected by the suspect. Most hacking tools and spyware rather unselectively collect all files created within specific time frame or all potentially relevant file types (e.g., PDFs or Microsoft Office documents). Similarly, an email investigation tool will likely collect all emails, containing a particular keyword or sent on a specified date, in an blanket and swift manner for further triage and analysis by crime investigators. Practically, within a remote cyber operation, a manual and careful selection of files, emails, or other digital evidence would oftentimes simply be impractically long and may expose the cyber operation to the suspect. Moreover, a suspect's device may be irregularly connected to the Internet, pressing cyber detectives to leverage the very first opportunity to quickly retrieve all available data, especially when dealing with violent criminals, where any delay may risk the lives of new victims. In contrast to the speedy and blanket cyber operations, a remote search may also be unnecessarily long, as pointed out by Quattrocolo (2020). For example, once police spyware is installed and the requisite digital evidence is successfully collected, the spyware remains for months or even years, sometimes being forgotten once the investigation is over. In sum, temporal, longitudinal, or other scope-related excesses of lawful hacking may negate all benefits of cyber investigations.

§ 2.9.2 Lack of Jurisdiction

The borderless and ephemeral nature of the modern Internet architecture gradually blurs the physical perimeter and geographical locations of data sought by law enforcement agencies. The ongoing evolution of technologies and soaring migration to multicloud or hybrid-cloud

environments has led to the so-called “loss of location” phenomenon. The loss of location describes a situation in which the sought data can transit through the wire of one country over milliseconds and then be gone in another one, or may fragmentally reside in several jurisdictions at once or even continually move from one datacenter to another across innumerable physical borders of sovereign states (Europol & Eurojust, 2019; Liguori, 2020). Even in comparatively trivial cases, where the key technical target of a lawful hacking operation is, for example, a suspect’s smartphone, it is still unclear what happens if the device temporarily crosses the national border of a foreign state or is connected to a foreign network in roaming. Picking up the discussion related to cloud-specific challenges elaborated in a previous section, it would require utmost creativity, technical eruditeness, and courage to attempt to determine whether a data center owner, its tenant or operator, or any subsidiary or external subcontractor thereof actually controls or co-owns the data in question and thus may be within the reach of territorial jurisdiction of a national court to authorize the lawful hacking of cloud-based infrastructure operated by criminals. Those examples create an almost unsolvable puzzle not only for law enforcement agencies, but also for lawmakers and governments. As fairly observed in a report by Privacy International:

> When conducting an extraterritorial hacking measure, government authorities must always comply with their international legal obligations, including the principles of sovereignty and non-intervention, which express limitations on the exercise of extraterritorial jurisdiction. Government authorities must not use hacking to circumvent other legal mechanisms – such as mutual legal assistance treaties or other consent-based mechanisms – for obtaining data located outside their territory. These mechanisms must

> be clearly documented, publicly available, and subject to guarantees of procedural and substantive fairness. (Privacy International, 2018, p. 38)

Resultingly, a perfunctorily performed cyber operation by law enforcement agencies may be punishable under the provisions of the national criminal law of the foreign country, as well as violate the unshakable principle of territorial sovereignty entrenched in international law (Brown, 2020). Ultimately, a lawful hacking campaign that transcends the permitted jurisdictional perimeter under the territoriality principle and consequently infringes the sovereignty of a foreign state, is poised to provoke a deterioration of diplomatic relationships or even unfold a political crisis (Schmitt, 2017). Worst, some states may take countermeasures in response to an act of cyber aggression, while others may reciprocate and commence large-scale cyber investigations on the infringer's territory, eventually leading to a spiraling multinational conflict and chaos (Ghappour, 2017). In sum, the obscure and blurred authority to conduct lawful hacking, caused by the imprecise territorial location of the targets, may have serious political consequences and legal ramifications, eventually discrediting lawful hacking in the eyes of politicians and lay people. The implications of international law in relation to jurisdiction over foreign-stored data or equipment are discussed in a detail in the Chapter 3 of this dissertation.

§ 2.9.3 Unreliable Digital Evidence

Challenges related to a proper, methodology-driven, and science-backed collection, preservation, and subsequent authentication of seized electronic evidence are elaborated in the previous sections of this chapter. The real-time nature and concomitant technical peculiarities of lawful hacking operations may predictably amplify and exacerbate those problems under certain circumstances (Bellovin et al., 2016). Some scholars and forensic experts have unequivocally expressed their frank apprehension that electronic evidence, seized by the means of lawful

hacking, may be accidently or even purposely altered by careless or over-enthusiastic cyber detectives:

> Hacking also leads to the collection of evidence in a way that makes it easy to tamper with or manipulate, meaning it can violate due process or fair trial rights. These rights can be used by digital rights defenders to challenge evidence obtained by hacking. Digital rights defenders can also push for the establishment of vulnerability disclosure processes, to increase transparency and reduce the likelihood of governments hoarding vulnerabilities. (Kumar, 2022, para. 5)

In a comprehensive and insightful review of the admissibility of electronic evidence obtained by lawful hacking, Sommer (2022) enumerated some widespread and generally recognized guidelines, standards, and frameworks utilized in the United Kingdom to govern the seizure and preservation of electronic evidence, such as the U.K. ACPO Good Practice Guide, the ENISA's Basic Guide for First Responders, or the U.K. Forensic Science Regulator's guidance. Afterwards, he raised over a dozen of judicious questions regarding the eventual compliance of lawful hacking operations with the foregoing frameworks in relation to the extraction, authentication, and preservation of electronic evidence following the applicable chain of custody requirements. He then stressed that, contrasted with traditional digital investigations providing physical control over the seized electronic equipment and usually having no pressing time limits, offensive cyber operations by law enforcement agencies are inherently secretive and are commonly conducted in a real-time mode. Eventually, compliance with the best practices in relation to digital evidence preservation and authentication become utterly complex or even technically unfeasible within cyber operations. Those concerns are particularly sharp when regarded though the lens of data volatility discussed earlier: live operations in cyberspace may

harvest an abundance of otherwise undiscoverable digital evidence that may, however, be eventually inadmissible in a court of law, unless the legislation finally addresses lawful hacking within criminal investigations and clearly states the dos and don'ts in relation to electronic evidence collection, preservation and management.

Another concern related to the reliability of the digital evidence stems from the inherently imperfect software design and the axiom-like impossibility of creating error-free software, be it for a simple digital breathalyzer or a sophisticated spyware toolkit (Bellovin et al., 2021). The miscarriage of justice becomes self-evident when police officers use spyware without first properly testing it for reliability, integrity, and consistency of the produced results, or for undocumented impact the spyware may cause on the suspect's device. Untested hacking software or backdoors may accidentally corrupt or lose the extracted data, as well as unwittingly destroy exculpatory evidence, make errors when gathering the timestamps of records, files, or events that actually may be crucial for the outcome of the investigated case. In continuation, Bellovin et al. (2021) report cases wherein—after installing spyware—the backdoored devices became vulnerable and could be easily compromised by external cybercriminals, who then exploited the backdoored machines for unlimited spectrum of computer-enabled crimes including, for instance, storing child pornography on the device. Whilst well-known digital forensics tools do follow certain processes of quality assurance and external auditing to prevent major bugs and errors in the code, spyware rarely follows the same path of rigorous reliability, quality, and results validity testing. Moreover, if spyware is developed by third parties, those parties will likely add strict non-disclosure and no reverse-engineering clauses into their software licenses, eventually selling an arcane black box. Depending on the jurisdiction, the accused may have a right to demand source code disclosure and its examination by independent experts for

algorithmic or other programming errors, as well as reporting inaccuracies as a matter of due process. Such a right is, however, rarely absolute and may be balanced with the interests of prosecution in keeping certain investigatory tools and hacking techniques under seal (Owsley, 2017). Eventually, in some borderline cases, where the only inculpatory evidence against the accused comes from a remote hacking operation, its fate may be callously decided by the extent of the spyware's reliability.

§ 2.9.4 Violation of Suspects' Rights

Lawful hacking is a prima facie intrusive and invasive method of digital investigation. If conducted improperly or without due precautions, it can seriously damage suspect's tangible and intangible property or violate its civil and human rights (Anstis, 2021). Depending on the jurisdiction, a suspect may enjoy a diversifying pallet of inalienable rights during the entire process of criminal investigation, prosecution, and court hearings. Those rights span from the right to protection from unreasonable searches and the right against self-incrimination to the right to suppress unlawfully obtained evidence, for example, evidence collected in violation of national or international law (European Digital Rights, 2021).

Illustratively, a 2016 report from Access Now opined that lawful hacking may violate, inter alia, multiple provisions of the Universal Declaration on Human Rights (UDHR), namely its articles 10, 12, 17, 18, 19, and 20 (Stepanovich et al., 2016). Among the prevailing concerns articulated in the report, Access Now mentioned possible violations of right to privacy, due process, and fair trial. The authors of the report argued that lawful hacking is far too sophisticated to be understood and, thus, reasonably expected by a layperson within a criminal investigation, as opposed to conventionally accepted physical searches of premises that have been rightfully exercised by police forces for over a century. Another pertinent concern

expressed in the report deals with the inadvertent chilling effect on the freedom of expression and thinking: being mindful that police officers may suddenly break into any computer or smartphone without notice, even the most innocent people will likely be disincentivized and refrain from keeping digital archives of their innermost memories, ideas, or feelings in the form of photographs, emails, notes, or electronic diaries. The oppressive big-brothering regime may also stifle the now-relaxed electronic communications and cheerful conversations with friends and relatives about potentially sensitive questions such as politics, religion, money, health, or sexual activities. Finally, the report drew readers' attention to the risk of amplifying mass surveillance that may be bolstered by lawful hacking:

> Government hacking in the context of surveillance is often more invasive than other forms of surveillance, and activities taken in pursuit thereof could grant nearly unfettered access to some of a person's most personal information, limited only by the imagination of the hacker and the design of the exploit. Traditionally, the incidents of government surveillance increase as the ability to conduct surveillance gets cheaper and easier. Government hacking may greatly reduce the cost of surveillance and lowers certain barriers to surveillance because it can take place remotely (Stepanovich, et al., 2016, p. 19).

Other scholars have voiced congruent concerns, including the possible interference of lawful hacking with the European Convention on Human Rights (ECHR) as asserted by Pool and Custers (2017), as well as the potential weakening of the presumption of innocence when intrusive methods are deployed to collect incriminating digital evidence by law enforcement detectives (Stoykova, 2021). Pool and Custers (2017) proposed that lawful hacking—being a highly intrusive instrument to conduct criminal investigations—must be judicially scrutinized

under three tests: the effectiveness test, the proportionality test, and the subsidiarity test, to assess the eventual compatibility of lawful hacking legislation with the provisions of ECHR Article 8. The first test examines whether the legislation is actually effective in achieving its underlying goals. The second test evaluates whether the nature, possible intrusiveness, and other collateral effects of the legislation are proportional with its context and do not create unnecessary risks to protectable rights and freedoms. Finally, the third test probes whether the same outcomes may be achieved with less intrusive and more privacy-friendly legislation (Pool & Custers, 2017). The proposed checks seem to be reasonable and well-balanced; they will be reviewed in further detail in Chapter 4.

What can be inferred from this section is that unless lawful hacking becomes a comprehensively regulated area of criminal law, setting inviolable borders for cyber operations and granting individuals cognizable rights and safeguards to duly shield their privacy and digital secrets in a reasonably acceptable manner, society will unlikely ever support the idea of intrusive cyber investigations by police. As wisely noted by Hon. Hazel Blears, the former U.K. Home Office Minister, "effective policing relies on the police having the confidence of the communities they serve, and this consultation gives the public an opportunity to contribute to the values and standards they expect of police officers" (Small, 2006, para. 3). That being said, to make lawful hacking socially and humanly acceptable, comprehensive legislation is required to regulate cyber operations in a simple, predicable, and safe manner.

§ 2.9.5 Violation of Third-Party Rights

In addition to the violation of suspect's rights by lawful hacking, it has been suggested that the uncontrolled usage of malware by police officers, searching for incriminating digital evidence during criminal investigations, may inflict material and large-scale harm upon innocent

third parties around the globe (Ohm, 2017; Pfefferkorn, 2021). At the time of writing, some scholars still conservatively focus their criticism on the hypothetically over-destructive capabilities of malware and investigators' lack of control over it. Other opponents of lawful hacking throw theoretical darts into police-managed malware, frequently citing unrepresentative or isolated cases, for instance, when instead of exfiltrating digital evidence, a poorly programmed piece of malware erased all data or even physically damaged a suspect's smartphone. The root cause of this regrettable misconception likely originates from the erroneous amalgamation of spyware used by law enforcement and malware used by cybercriminals. Commonly, the latter is purposely built to be highly contagious and to have viral self-propagation capabilities to spread over millions of devices in an attempt to infect as many devices as possible. Those attributes of malware are, however, largely inapplicable to the special-purpose police spyware, which is usually designed to remain invisible and undetected for as long as possible, being as nonharmful as practical. Moreover, modern-day police spyware commonly has advanced capabilities to securely remove itself from a compromised system once the investigation is over, without leaving digital traces or suspicious artefacts that could uncover the police investigation.

Another spyware-related trigger of trepidation, popular among opponents of lawful hacking, derives from the reportedly over-intrusive capabilities of police spyware. Some publications cite, among other things, the permanent interception and real-time recording of sound and video streams from the compromised device's microphone and camera, which may unintentionally capture live discussions or images of innocent third parties unrelated to the investigation. Whilst such technical features are indeed available in modern police spyware, they are virtually never used in a permanent mode to, inter alia, avoid detection by the suspect. For

example, a permanently enabled smartphone's camera or microphone that sends a live data stream to a remote server will inevitably deplete the smartphone's battery charge in a couple of hours or even faster. Consequently, the suspiciously fast consumption of device's battery may serve as a red flag and reliable indicator of the device's compromise to the suspect, thereby spoiling the entire cyber investigation. Despite the discernible tendency to overstate certain risks of police spyware, a detailed technical guidance on police spyware deployment and usage by cyber detectives, namely strict requirements of proportionality and harmlessness, should become an integral part of lawful hacking legislation.

The next set of foreseeable risks to third parties originates from an unintentional infringement of third-party intellectual property rights. For instance, cyber operations by police experts may regularly rely on carefully planned spear-phishing attacks, justified by their efficiency and relative simplicity in certain cases (Burns et al., 2019). Spear-phishing attacks commonly imply a forged email and fake website ostensibly belonging to a well-known brand or organization, ranging from Microsoft to Greenpeace. Such attacks almost always incorporate some copyrighted content and registered trademarks, obviously without authorization from the intellectual property owners. Within a broad extrapolation, one may attempt to argue that good-faith usage of copyrighted materials within lawful hacking may be covered by one of the exceptions provided by the fair use doctrine and, thus, is lawful. It would be difficult to contest, however, that within police investigations, a systematic misuse of a globally recognizable trademark may constitute a peculiar vector of trademark dilution (Beebe et al., 2019). Moreover, if regular citizens realize that the electronic communications of their favorite brands are frequently falsified and actually come either from cyber gangs or law enforcement agencies setting investigatory traps, the citizens may subconsciously lose their trust in such

communications and eventually avoid any content coming from those brands. This mental shift will undoubtedly inflict palpable reputational and financial harm upon the trademark owners, who will unlikely agree to sacrifice their goodwill on the altar of criminal justice. Whilst even private cybersecurity companies start taking serious precautions in phishing attack simulations and anti-phishing awareness exercises to avoid infringement of third-party intellectual property (Stacho, 2022), law enforcement agencies should be held to a much higher threshold of accountability, diligence, and care.

Even more problematically, lawful hacking may purposely or unwittingly interfere with, or pierce through, a third-party IT infrastructure—ranging from a desktop computer owned by the suspect's employer or a shared infrastructure in a multitenant cloud environment—when searching for, or extracting, digital evidence requisite within a criminal investigation. Unescapably, such tactics generously pour gasoline on the flame of scholarly debates over the risks of lawful hacking to IT infrastructure and electronic equipment owned or operated by third parties. The multifaceted side effects of lawful hacking become particularly disquieting when regarded through the prism of the presumably uncurbed "finishing expeditions" of law enforcement agencies. For instance, it has been hypothesized that a governmental agency may break into a corporation under the pretext of investigating a serious criminal offense committed by one of its employees, whilst in reality being interested in electronic evidence of tax evasion committed by the corporation. The risk skyrockets when dealing with law firms that, whilst of course not immune from being rightfully charged with serious offenses committed by their employees, store immeasurable volumes of privileged and otherwise protected information. The archives of large law firms may be a treasure trove for police officers, who may aptly exploit them as an ever-green source of actionable intelligence to streamline new investigations based on

previously unknown facts, thereby enabling prosecutorial authorities to massively bring charges against the law firm's clients in an ultra-expediated and effortless manner. The foregoing equally applies to many other specially regulated professions or entities such as banks, which may suddenly become a key target of lawful hacking to proactively spot money laundering or violations of sanctions under the color of a narrow criminal investigation pending against a bank employee. Such overtly impermissible fishing expeditions, despite their undeniable benefit for suppression of crime, will irreparably harm public's trust in justice and erode the integrity of the rule of law.

One last concern about third-party rights infringements within lawful hacking relates to the excessive usage of zero-day vulnerabilities or novel hacking techniques that may become available to police officers. After a lawfully conducted cyber operation relying on a zero-day vulnerability in a very popular software or hardware product is successfully completed, it may trigger an unhealthy investigatory appetite among the officers. Cyber detectives may have an irresistible temptation to silently expand their investigation to all other "villains" whose IT infrastructure is also vulnerable to the zero-day flaw and who—for some reason—could not have been lawfully hacked in the past (Internet Society, 2020). The foregoing tellingly explains the necessity of thoroughly regulating and supervising lawful hacking operations to prevent opening a Pandora's box of uncontrollable and emotional investigations, fishing, or punitive expeditions in cyberspace.

§ 2.9.6 Cyberwarfare Misappropriation

In 2016, a remarkable collection of armor-piercing exploits, mostly targeting zero-day vulnerabilities in Microsoft products, was reportedly stolen from the National Security Agency (NSA) by sophisticated cybercriminals: threat actors behind the high-profile attack leaked some

of the exploits and launched a public auction to sell others (Richards, 2017). Two years later, the misappropriated cyberwarfare, namely the infamous “EternalBlue” exploit, has been utilized in targeted ransomware campaigns against American cities and essential objects of the Critical National Infrastructure (CNI), including water supply stations, oil and gas pipelines, hospitals, airports, and railways (Perlroth & Shane, 2019). Other large-scale hacking campaigns relying on the same cyberweapon, misappropriated from the NSA, have been allegedly performed by various cyber adversaries backed by hostile nation states, causing billions of dollars in direct damages. Whilst the NSA and the FBI declined to comment on the deplorable incident, this story provoked nation-wide public outrage, calling for the regulation or even total prohibition of advanced cyberwarfare development by governmental agencies at the expense of taxpayers.

One year later, in 2017, another ground-trembling security incident of an even higher amplitude and scale shook the Central Intelligence Agency (CIA), when Wikileaks released a report, known under the codename “Vault 7,” documenting the theft of over 9,000 confidential files and documents from the CIA (Culafi, 2020). The exposed dump contained, among other things, numerous hacking tools and exploit kits for zero-day vulnerabilities in iOS, Android, and various Microsoft products, tailored to invisibly compromise smartphones, computers, and even smart TVs without raising the victim’s suspicion. Evidently, the disastrous CIA leak originated from insufficient and flawed internal security controls at the agency, which eventually led to the compromise and misappropriation of top-secret cyberwarfare. Worse, the CIA was allegedly unaware of the leak until the scandalous *exposé* by Wikileaks. After five years of investigation, a CIA-employed programmer was eventually found guilty of stealing the cyberwarfare in question from the CIA and handing it to WikiLeaks afterwards (Ropek, 2022), raising even more questions regarding how one single, low-ranked employee could abscond with the crown jewels

and other highly classified information without being detected. Whilst this research does not cover hacking by national intelligence agencies, the above-mentioned examples may well occur one day with national police that likely have even less resources to protect their cyber tools and instruments compared to the NSA and the CIA.

Foreseeably, the striking NSA and CIA gateways have been mentioned in countless media and scholarly publications advocating against lawful hacking by governments in light of their flagrant and outrageous inability to safeguard access to their own cyberwarfare instruments. Consequently, legal scholars (Brown, 2020) and nongovernmental organizations (Privacy International, 2018; Internet Society, 2020) have attracted the attention of lawmakers to the far-reaching risks of governmental cyberwarfare misappropriation by sophisticated threat actors and the subsequent domino effect on cyberattacks against individuals, enterprises, governments, and CNI objects. Hence, as a prerequisite to cyber operations, lawful hacking legislation should seamlessly integrate and prescribe a threat-aware and risk-based data protection strategy, holistic set of continually improved information security controls, zero-trust and defense-in-depth architecture, as well as ongoing internal and external audits and employee awareness training.

§ 2.9.7 Negligent Subcontractors

It is hard to image a law enforcement agency that could handle the entire cycle of cyber operations without hiring external vendors or subcontractors for a broad variety of technical tasks, spanning from training of its personnel and consulting to purchase of exploits, hacking tools, zero-day vulnerabilities or sophisticated spyware. Whilst the partial outsourcing of lawful hacking to external vendors undoubtedly brings cost-efficiency, agility, and other operational advantages, it certainly carries its own risks. Those risks are bifurcated into two main branches: the first covers the carelessness and negligence of subcontractors, whilst the second addresses

deliberate or reckless misconduct by subcontractors, their employees, or shareholders. Both issues are equally important and are detailed below.

Historically, the first major data breach of a governmental subcontractor involved into a form of lawful hacking can be traced back to 2014, when Gamma Group—a private European company supplying governmental clients with spyware for criminal investigations—was hacked (Blue, 2014). Over 40 gigabytes of highly confidential data, including the source code of the notorious "FinFisher" spyware, were stolen and leaked online. One year later, an Italian company, tellingly named "Hacking Team," was actually hacked itself. Hacking Team, then the leading private operator of hacking and digital surveillance services for governments, suffered an overwhelmingly gigantic and embarrassing data breach: over 400 gigabytes of its top-secret and internal information were leaked publicly, including but not limited to its customers lists, the emails of executives, backups, and the source code for their hacking tools and spyware (O'Neill, 2019). Alarmingly, the ensuing journalistic investigations uncovered that the famous hackers-for-hire had not shunned work with allegedly repressive regimes targeting journalists and human rights activists in their cyber operations, under the pretext of criminal investigations. The Hacking Team incident attracted broad attention to the information security of governmental subcontractors involved in hacking operations, as well as to the ethics and legality of such missions carried out in cyberspace. Within this context, one may also question the eventual duration of digital evidence storage by subcontractors and by their own subcontractors: if sensitive data is not immediately and securely deleted upon a transfer to competent authorities once the investigation is over, the risks of a data breach soar. Subcontractors will become a goldmine for cyber mercenaries hired by hostile nation states or organized crime. Moreover, sophisticated cyber-threat actors may effortlessly penetrate into a poorly protected governmental

subcontractor and inject a hardly detectable backdoor into the source code of police spyware used in criminal investigations, eventually gaining the keys to the entire kingdom of lawful hacking. Thus, every new target of police investigation will automatically fall under the invisible control of cybercriminals or their more dangerous and influential masters. Obviously, one single case of spying over police cyber detectives may radically shift public opinion about lawful hacking into unfixable hostility. In continuation, the more recent data breach of Israeli mobile investigation company Cellebrite, serving law enforcement agencies from dozens of countries, once again convincingly demonstrated that insecure suppliers and subcontractors are the Achilles' heel of law enforcement—after over 900 gigabytes of confidential data were leaked (Cox, 2017).

Following the thunderstriking success of "Encrochat" and "ANOM," undercover operations of unparalleled depth and scale, which have been artfully run by joint taskforces of the Western law enforcement agencies (Zagaris & Plachta, 2020; Cox, 2022), the cartels of organized crime and transnational drug dealers—targeted by the operations—became paranoid. Upon realizing that law enforcement agencies have been actively leveraging advanced cyber investigations, organized crime will now generously pay for any actionable information about ongoing or future cyber investigations by police. Organized crime will likely exploit the purchased information to identify and then assassinate undercover police agents, neutralize the backdoored devices of its members, or even attempt to conduct perfidious counterintelligence operations by transmitting deliberately false and misleading information over the compromised devices silently monitored by unwitting police investigators. Therefore, in view of the mounting conflicts in cyberspace and the foreseeable increase of attacks against police units, data protection by vendors and suppliers becomes extremely critical.

Importantly, vendor's negligence is not restrained to data protection questions, but may also encompass service or product quality. In continuation of the Encrochat operation, it is worth mentioning here that the spyware implanted into Encrochat cryptophones was severely criticized by experts for allegedly having countless technical deficiencies, presumably coming from numerous bugs in the spyware source code and its flawed architecture (Goodwin, 2022). Consequently, the obtained electronic evidence has been vigorously stigmatized by criminal defense lawyers as unreliable, untrustworthy, and thus inadmissible in court, calling out a mass misattribution of serious crimes and wasting a considerable amount of expert witnesses' time in acrimonious court battles. At the time of writing, animated debates over the admissibility of the Encrochat's digital evidence are occurring in many European courts, though in some criminal proceedings, the prosecution managed to escape this cumbersome process by securing a guilty plea from the suspects (Roberts, 2022). Despite that the underlying technical details of the Encrochat operation are not publicly known, it is reasonable to hypothesize that some external companies or experts participated in designing, developing, or testing the spyware in question, evidencing that the substandard quality of subcontractors' work may be fatal for successful prosecution of criminals.

Another facet of operational risk emanating from subcontractors derives from innate human weaknesses, namely deviant and malignant behavior. When outsourcing any component of cyber operations to privately held entities, a government may spectacularly slip on an illicit or insidious behavior by the individual employees of their commercial suppliers. Plausibly, motivated by money and greed or forced by blackmailing and threats, an employee may be a secret recruit of a foreign intelligence or organized crime, leaking highly confidential information and eventually ruining an entire investigatory campaign. Inversely, a modern-day

Robin Hood employee, driven by subjectively laudable and noble motives, may suddenly decide to expose sealed documents regarding governmental operations conducted in cyberspace, believing them to be illegal, immoral, or otherwise deserving of public exposure. Whatever the original causes of the information leakage, its outcomes may cause irreparable short- and long-term harm to how law enforcement functions, endanger the lives of innocent citizens and undercover police officers, and erode public trust in the concept of lawful hacking in criminal investigations.

Finally, shareholders or board members of governmental subcontractors may have interests that diverge from, or conflict with, those of their state customers, and thus eventually attempt to illicitly exploit information or intelligence about the targets and techniques of lawful hacking entrusted to them. Background checks and continuous due diligence rarely help prevent deviant behavior in the future, leaving such high-profile threats without a silver-bullet solution. Notably, to disempower the bloodthirsty hydra of subcontractor risks, Anstis (2021) developed and proposed a comprehensive framework for transparently regulating public–private relationships with technology vendors involved in lawful hacking or surveillance operations by the government. The framework can serve as a good example of the baseline security controls that should be imposed upon police subcontractors by the virtue of lawful hacking legislation.

§ 2.9.8 Zero-Day Proliferation

Almost a decade ago, in their milestone publication on lawful hacking—discussed in the previous sections—Bellovin et al. (2014) questioned whether research for zero-day vulnerabilities and their subsequent exploitation by governmental actors would disincentivize software vendors from building more secure software, as well as have a chilling effect on software vulnerability patching by users. Similar concerns were recently echoed in a 2018 report

published by the Center for Internet and Society (CIS; Pfefferkorn, 2018). Theoretically, private technology companies and their customers may indeed be disincentivized to undertake extra efforts to keep their software and operating systems up to date, knowing that law enforcement or criminals with stolen cyberwarfare will sooner or later break in, despite their best efforts to prevent the attacks.

Whilst zero-day proliferation was a reasonable and dominant concern in 2014, it is unlikely to be of a significant importance in 2022: modern-day cyber adversaries may select from *à la carte* abundance of publicly known, widespread, and unpatched vulnerabilities to swiftly break into organizations without spending bitcoins on expensive zero-days (Cybersecurity and Infrastructure Security Agency, 2021). Furthermore, in 2022, law enforcement agencies probably represent one of the smallest players on the global zero-day market, being considerably understaffed and underfunded to conduct such costly activities in a large-scale manner (Moloney et al., 2022). Importantly, this research—as highlighted in the first chapter of this dissertation—does not cover national security and intelligence agencies that may have incommensurably more resources and needs for zero-day vulnerabilities. Technically, successful exploitation of zero-day vulnerabilities in corporate networks can be significantly reduced by a multilayered cyber-defense enhanced with an automated incident detection and response program (Sawant, 2018; Radhakrishnan et al., 2019; Yadav et al., 2019). Hence, the researcher considers that the old concern over disincentivized users and demotivated vendors, unwilling to build secure software because of the exploitation of zero-day flaws by law enforcement agencies, has been naturally dispelled by the evolution of cybercrime and the cybersecurity industry.

Interestingly, Bellovin et al. (2014) also inquired whether law enforcement agencies, as a matter of public policy, ethics, and law, should participate in the grey market for zero-day vulnerabilities, buying cyberwarfare from unknown sellers that conceal or disguise their identities, thereby contributing to the growth, and de facto legitimization, of underground commerce. This murky aspect of zero-day trading is visibly trickier and sharper today that it was in 2014, given that most payments for cyberwarfare and related goods are usually made in untraceable cryptocurrencies. According to the U.S. Office of Foreign Assets Control (OFAC), payments made in bitcoins and other cryptocurrencies may constitute a violation of U.S. sanctions, as the true recipients of funds are unknown and usually cannot be ascertained with reasonably certainty (OFAC, 2021). Hence, law enforcement agencies may have no choice but to violate the sanctions to acquire the tools and zero-day vulnerabilities requisite for lawful hacking, creating a legal controversy and a political paradox. This idea was recently revived and further expanded by Schneier (2018), who further questioned the indirect promotion, cultivation, and legitimization of the grey market for zero-day vulnerabilities and hacking tools by law enforcement. He warned that cyber weapons dealers will quite likely sell their goods to other buyers in parallel, including but not limited to professional cyber mercenaries backed by hostile states, organized crime syndicates, or terrorists. This fact intriguingly raises a thought-provoking dilemma of whether paying for zero-day vulnerabilities ultimately finances the hostile threat actors and furthers their development of hazardous cyberwarfare that will eventually end up attacking national banking infrastructure, CNI objects, and the government, whereas the latter actually allocates taxpayer's money to fertilize the technical capabilities of the threat actors.

Unsurprisingly, the sharp angles of acquisition and in-house research for zero-day vulnerabilities by governmental agencies remain highly controversial and are intensively debated

by legal scholars, cybersecurity experts, and governmental agencies (Liguori, 2020). The researcher acknowledges that unregulated development, utilization or commercialization of cyberwarfare, which exploits zero-day vulnerabilities impacting major software or hardware vendors, may and will likely have unpredictable and undesirable consequences. As a possible solution, countries may consider implementing a holistic process to regulate zero-day vulnerabilities acquisition, usage, and subsequent disclosure to vendors. The Vulnerability Equities Process (VEP) implemented in the United States may exemplify such process. Whilst being a legally nonbinding charter, the VEP addresses the disclosure of zero-day vulnerabilities by the U.S. federal government in attempt to equilibrate the rights and expectations of vendors, society, and the government in a fair and balanced manner (Schaake et al., 2018). Procedurally, a VEP-inspired process should probably be incorporated into national legislation on lawful hacking to make the process and its provisions legally enforceable. Otherwise, it may face similar critique and reproaches as the VEP program in the United States for not being legally binding or enforceable, thus raising questions over its practicality and eventual utility (Thompson, 2021).

§ 2.9.9 Smoke-Screen Operations

Another possible collateral effect and a conceivable risk of lawful hacking is represented by smoke-screen cyberattacks. Such attacks may be calculatingly conducted by sophisticated cyber threat actors, aiming at perfidiously framing law enforcement agencies as the authors of illicit hacking campaigns. Once it becomes a public knowledge and commonly accepted dogma that law enforcement agencies may hack individuals and enterprises within criminal investigations, the agencies will likely end up in the crosshairs of global cyber gangs. Once IT infrastructure owned or operated by a law enforcement agency is compromised, it can be

exploited as a proxy platform from which to launch destructive cyberattacks against innocent third parties, ranging from local journalists and politicians to CNI objects in hostile states, framing not just the hacked agency but the entire country. Proving the innocence will be an arduous and time-consuming task. Other cyber threat actors, having purely commercial and pragmatic motives, may simply exploit backdoored police networks to complicate cyberattack investigations and make their attribution virtually impossible, with similar consequences. Eventually, law enforcement networks will become a magnet for sophisticated cyber wrongdoers.

In light of the surging cyberattacks that purposely target law enforcement agencies with a quite impressive success rate (Kovacs, 2020; Resecurity, 2021), a considerable number of backdoored police networks and systems may be placed for sale on the Dark Web to be later exploited as proxies, creating smoke screens for hacking campaigns. Making the situation even worse, the breached agencies' denial that they are behind such attacks can actually spiral into a new trend of state cyber-terrorism, whereby dictatorial regimes will openly launch cyberattacks against rival states and then simply blame foreign hackers (Schmitt, 2017). Some villain players, familiar with the game theory, may even go one step further in their perfidious recriminations by asserting that the victims have orchestrated the attacks themselves to cunningly accuse them. Hence, a reliable and evidence-backed investigation and subsequent attribution or cyberattacks, as well as lawful countermeasures to the attacks, will become a nearly unfeasible and highly politicized task (Delerue, 2020).

§ 2.10 Less Intrusive Alternatives to Lawful Hacking

As demonstrated in the previous sections, lawful hacking carries a wide spectrum of legal, technical, and operational risks, and thus should be treated with the utmost care,

precaution, and diligence. Likewise, lawful hacking should not be used by police as an all-purpose or catch-all solution to solve serious crimes when less intrusive or more cost-efficient alternatives are available. Unthoughtful or unselective deployment of lawful hacking operations may be unreasonably expensive and unjustifiably intrusive, as well as expose proprietary hacking techniques or zero-day vulnerabilities to criminals and security researchers, eventually causing more harm than good. Several complementary, comparatively unintrusive, and less resource-intensive alternatives to lawful hacking are discussed below to paint a comprehensive picture of lawful hacking, prior to delving into a review of the existing lawful hacking legislation in Chapter 3.

§ 2.10.1 CCTV Surveillance

Large cities and even small villages are becoming increasingly overequipped with lawfully installed CCTV video monitoring systems, operated both by governmental bodies and countless private actors. Streets, public transportation, office buildings, and bars are pervasively equipped with continuous video monitoring for safety reasons. For instance, in London, amid over 500,000 active CCTV systems, an average citizen is estimated to be tracked by 300 cameras every day (Claburn, 2022).Whilst the permitted area and hours of surveillance, duration of video storage, and other operational details of CCTV monitoring may vary considerably from one jurisdiction to another, all megapolises and many smaller cities are lawfully filming residents in a permanent mode to prevent crime and for other legitimate purposes expressly authorized by applicable law.

Eventually, if the suspect's identity is known, before executing a search and seizure warrant targeting its digital equipment, it is worth preparing the ground for decrypting suspect's electronic devices that may be confiscated for investigation. In many cases, the chances that the

suspect has been accidentally filmed by a lawfully deployed CCTV surveillance system (e.g., while entering a password into a laptop or iPad while sitting in a hotel lounge or restaurant) are high. Even a low-quality video may reveal distinguishable keystrokes that can be used to reconstruct the secret passphrase. Cyber detectives should, however, rigorously plan the operation, considering the mobile forensics pitfalls and challenges elaborated in Chapter 2 of this dissertation. For instance, data volatility and evidence authentication may be crucial: merely entering a captured passcode into a smartphone and then leaving it for a few days until the digital forensic lab has a slot is a reliable way to lose valuable electronic evidence or make it inadmissible in court. In continuation, a request for CCTV recordings from surveillance operators should normally be accompanied with a warrant, subpoena, or other jurisdiction-specific legal instrument to ensure the legality of the process and the eventual admissibility of the digital evidence in a court of law. In sum, certain digital investigations dealing with device encryption may have much simpler, faster, and less costly solutions than a lawful hacking operation in cyberspace.

§ 2.10.2 Undercover Investigations

Collection of incriminating digital evidence within criminal investigations is not always an intrusive or invasive process. A prudent undercover investigation can brightly illuminate the inculpatory evidence concealed in the shadows and penumbras of the Internet, without breaking into any private systems or electronic devices. For example, when investigating an underground network of pedophiles, an undercover police officer may infiltrate the criminal circle to stealthily collect information and intelligence about any past or future offline activities of the illicit circle members. In contrast to online interactions, offline events may expose not just the ordinary consumers of prohibited content, but also the masterminds behind the human trafficking and

child exploitation networks, those who actually pull the strings to produce and proliferate the harmful content around the globe.

Naturally, an undercover investigation may take several weeks or even months and require painstakingly planned efforts from a team of specially trained police detectives. However, a lawful hacking operation will probably require a comparable duration to silently take control over numerous remote devices, likely consuming even more resources and hours of experts' work. Therefore, despite the growing digitalization of criminal investigations, classic online and offline methods of unmasking perpetrators of serious or organized crime should not be discounted or disregarded by law enforcement agencies.

§ 2.10.3 Social Engineering and OSINT

Social engineering relies on various psychological and manipulative techniques to exploit various human weaknesses, such as gullibility or naivety, sometimes successfully bypassing all layers of a sophisticated cyber defense and accessing confidential information from an organization without utilizing any traditional hacking techniques (Wang et al., 2020). During a social engineering attack, the erudite attacker "uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. [The attacker] may be able to piece together enough information to infiltrate an organization's network" (Cybersecurity and Infrastructure Security Agency, 2020, para. 1). Under certain circumstances, social engineering may and should substitute lawful hacking operations, as a faster and more cost-efficient investigative technique.

Socially deviant offenders are prone to habitual human weaknesses and emotions, including greed, anger, arrogance, and fear. Moreover, some offenders may imprudently enjoy surfing and communicating on social networks, interacting with their school friends, ex-partners,

military comrades, or even gym acquaintances, either under a pseudonym or even incautiously using their real name. Enhanced with Open-Source Intelligence (OSINT) investigation techniques, social engineering may be a potent weapon in the cyber arsenal of law enforcement agencies, capable of ferreting out who is hiding behind a fancy pseudonym based on, for example, its connections, group memberships, tags on photos, likes, or comments. In other cases, already-identified suspects may communicate with their accomplices, suppliers, or clandestine clients via online chats or dashboards, sometimes using steganography or specially encoded keywords to disguise the true meaning of their messages. Using a covert identity and being equipped with pre-existing intelligence or information gathered via OSINT research, an experienced police detective may cautiously reach out to the suspect and try to establish a relationship of confidence and trust or, contrariwise, induce negative emotions and lead the angry or frustrated suspect to commit some self-incriminating or self-exposing errors. For instance, after being told a convincing legend, a temporarily blinded suspect will agree to selling or even gifting illicit goods to an "old friend," carelessly inviting the latter to the suspect's house or even to a secret warehouse where the contraband is stored. In another hypothetical example, police officers may imitate a random ex-buyer of criminal services or outlawed products, claiming the poor quality of the deliverables and demanding reimbursement. Eventually, the irritated or frightened suspect may disclose identity-revealing information or expose other actionable intelligence, under simmering emotions.

Occasionally, the ultimate success of a criminal investigation is simply wrapped into revealing the identity or whereabouts of the suspect. Under such simple set of circumstances, police officers may try to interact with the anonymous perpetrator online, who may excel in utilizing anonymous messengers, VPNs or other identity-concealing mechanisms. In everyday

practice, however, a VPN may not always be enabled or may suddenly stop working, widely opening a door for creative social engineering campaigns aimed to expose the suspect's identity. Technically, a VPN may even be taken down by police for a several minutes to expose the real IP address of the suspect. For example, if the suspect is caught off guard by a provoking, insulting, or exciting message, the suspect may unthinkingly click on a credibly looking hyperlink, imitating a famous website or governmental web resource. In reality, the website will be under the control of police officers, who will immediately get the IP address of the suspect and probably collect other indicators of that person's real location. Sometimes, when the suspect travels between numerous, albeit known shelters across different countries, one imprudent click may expose suspect's current time zone, suggesting its possible whereabouts and facilitating the arrest.

Obviously, the foregoing hypotheticals are simplified examples of social engineering campaigns, which oftentimes may require a painstaking preparation of a multistage operation, as well as simultaneous involvement of several police officers to thoroughly elaborate a trustworthy legend and then impeccably execute the operation. The aforementioned examples, however, tellingly illustrate how a set of non-hacking techniques of social engineering, enhanced with OSINT information gathering, can elegantly substitute costlier lawful hacking campaigns and produce the same or even better results. Importantly, all covert operations usurping the real identities of any existing persons shall be planned with extreme precautions and in strict compliance with applicable law. Likewise, cyber investigators shall avoid any prohibited tactics, such as entrapment (Hill et al., 2018), otherwise, they will not just spoil the operation but may also face sanctions themselves.

§ 2.10.4 Financial Rewards for Information

The longstanding practice of paying financial rewards for the whereabouts of dangerous criminals can be elegantly combined with financial rewards for their passwords or passcodes, when those are, or may be, required within a criminal investigation to unlock an electronic device. As discussed in the previous section, most criminals are habitually prone to common human weaknesses and, thus, make trivial mistakes, for instance using identical passwords everywhere or boasting about their criminal "feats" to their friends or partners. Others may recklessly enter passcodes into their smartphones whilst being surreptitiously or unintentionally watched by friends, accomplices, or other presumably trusted parties. Eventually, a number of acquaintances, relatives, or lovers, may know the magic word to unlock a mobile device with gigabytes of incriminating data. For obvious reasons, law enforcement agencies cannot ignore such unmissable opportunities.

Therefore, when the identity of the offender is reliably established, without doubts, the authorities may publicly offer a financial reward for valid passwords to the offender's smartphones, laptops, online accounts, or other digital systems that may contain information valuable for the investigation. Additionally, immunity from prosecution may be offered to accomplices, aiders, and abettors, who decide to collaborate with the prosecution, when doing so is not be contrary to the public policy or fundamental interests of the victims. Despite that this method is narrowly applicable and requires, inter alia, the offender to be arrested or otherwise legally incapacitated and unable to change relevant passwords or delete relevant online accounts, in some cases the keys to the digital realm of serious crime will arrive in less than 24 hours, saving taxpayers money that would otherwise be spent on weeks of costly lawful hacking in cyberspace.

§ 2.10.5 Dark Web Research

In the misty realm of modern cybercrime, even the "untouchable" senior members of criminal cartels and transnational gangs, recidivists, and other dangerous criminals have no immunity, and thus they may occasionally fall victims to large-scale hacking or untargeted ransomware campaigns, like anybody else who is connected to the modern Internet. With billions of compromised credentials, accounts from online services and public websites readily available for sale on the Dark Web (Hope, 2022), law enforcement agencies may harvest this valuable data for criminal investigations. Moreover, given that criminals may also have bad habits, such as password reuse, even a single incident in the past may unlock many doors, hiding the darkest secrets of organized crime. Data stolen from criminals, or even access to their backdoored electronic devices, may also be purchased on the Dark Web from unwitting cyber gangs that obviously did not specifically target those victims.

There are, however, certain legal considerations and practical precautions to consider for law enforcement when acquiring passwords or other intelligence on the Dark Web, even if the purchased intelligence is not designed to be later adduced in a court of law. Firstly, payments in cryptocurrencies may trigger problems already described in the zero-day proliferation section above, such as the violation of sanctions. Secondly, the legality of utilizing stolen credentials to extract digital evidence from remote systems may likewise be questionable, to put it mildly, and vary from one jurisdiction to another. Some jurisdictions have even flatly prohibited prosecution from using stolen information as inculpatory evidence in court; however, it is unclear whether the ban covers the purchase of stolen information to be used as intelligence for further investigations. Possible infringements of third-party rights, as earlier discussed, may equally pose a problem. For instance, using someone else's credentials to log in to webmail may violate

the terms of service of the webmail provider. Thirdly, in a rare but conceivable case of purchasing access to compromised and backdoored devices of the suspect, additional attention must be paid to the eventual admissibility of the digital evidence collected in such an operationally unorthodox and legally ambivalent manner. In sum, the acquisition of incriminating electronic evidence on the Dark Web is a promising but nascent trend, largely unsettled or even unseen in many jurisdictions. Its technical delicacy and legal subtleties require supplementary regulation by lawmakers to unambiguously establish the permissible borders of such operations. It may, however, be a great extension of, or even replacement for, lawful hacking in some cases.

§ 2.11 Chapter Two Summary

Being the largest part of the dissertation, Chapter 2 started by discussing the purpose and methodology of the literature review conducted herein, explaining its fitness for the research purpose and its suitability to answer the three research questions. Next, the chapter concisely reviewed why electronic evidence is indispensable and crucial in contemporary investigations of organized and serious crime. Then, a broad spectrum of technical, operational, and legal obstacles to the collection and seizure of electronic evidence was discussed through the prism of possible solutions. In continuation, various examples of existing legislation—aimed to overcome the foregoing problems, pitfalls and challenges—were discussed, with the eventual conclusion that they are narrowly applicable in practice and cannot substitute lawful hacking. Ultimately, lawful hacking was found to be a more cost-efficient and technically effective way to seize electronic evidence when investigating serious and organized crime. Afterwards, to ensure a two-sided and impartial approach to the research, a comprehensive list of risks and threats stemming from lawful hacking was produced and discussed. Finally, a short compilation of less intrusive

technical means for the collection of incriminating digital evidence within criminal investigations was provided to suggest that, under a narrow set of circumstances, lawful hacking can be efficiently, although only partially, replaced by less intrusive technical means.

3. CHAPTER THREE

§ 3.1 Research Method Rationale

Following the definitions provided by Oun and Bach (2014), this research can be classified as applied and practical, aiming to synthesize the analyzed data to produce an actionable framework that would have a straightforward practical application, as explained in Chapter 1one of this dissertation. Likewise, as already elaborated in the first chapter, this research uses a qualitative methodology and exploratory case study design that relies on the document analysis method to collect and analyze data. Bowen (2009) defines the process of document analysis as "a systematic procedure for reviewing or evaluating documents – both printed and electronic (computer-based and Internet-transmitted) material" (p. 27), indicating that "document analysis is particularly applicable to qualitative case studies" (p. 29). Whilst admitting that document analysis has been prevailingly used in combination with other research methods (e.g., with structured and unstructured interviews or focus groups), he draws the reader's attention to the fact that document analysis can be flawlessly implemented as a standalone research method. Moreover, he expressly indicates that there are specific research cases wherein document analysis is the only appropriate research method because in-person interviews, as well as other forms of live interaction with human subjects, would be impractical, unreliable, or unrepresentative.

§ 3.2 Research Method Validity and Reliability

Whilst advocating for the document analysis research method, Bowen (2009) prudently cautions that document review is prone to certain weaknesses. Among its possible drawbacks, he

names the inaccuracy or even fallacy of documents coming from untrusted, unverified, or unverifiable sources, as well as researchers' frivolous interpretations of a document in an incorrectly framed context that eventually distorts the original meaning or underlying message of the document, alongside the possible bias of a researcher in the selection of documents that would lead to a foregone conclusion. Bowen further underlines that when performing document analysis, the quality of the chosen documents crucially outweighs their quantity. In the end, he concludes that with a set of reasonable methodological precautions designed to prevent the foregoing logical fallacies, cherry picking, and inaccuracies, document analysis is a reliable, efficient, and effective method by which to conduct credible scientific research (Bowen, 2009).

To mitigate, or at least to minimize, the above-mentioned risks to the reliability and validity of the document analysis method, this research (i) collected the data from peer-reviewed scholarly articles, official websites of governmental bodies or agencies, from the official websites of accredited non-governmental organizations, and from known scholars and subject-matter experts recognized in their domain; (ii) perused and examined the documents in their original context and environment by, among other things, analyzing the timelines of the documents' publication and ascertainable relationship both with the preceding and succeeding publications from the same source or by the same author, reviewing other scholarly publications citing or commenting on the documents in question, and searching for more recent publications or documents that could repeal and novate the inspected documents; (iii) analyzed diversified sources and authors of documents so as to maintain a fair equilibrium of opponents and proponents of lawful hacking, illuminating both its key risks and principal benefits to the most balanced extent possible; and (iv) compiled the documents and other literature studied during the

research in the Bibliography section of this dissertation, so that they can be easily and transparently identified, consulted, and critically examined by the reader.

Congruent with the Bowen's cogent arguments, other scholars have also been promoting document analysis as a valid and reliable scientific research method, both when it is leveraged as a standalone method and when it is just one of mutually supporting research methods. For example, Ahmed (2010) says that document analysis "is just as good as, and sometimes even more cost effective, than the social surveys, in-depth interview or participant observation" (p. 2). Ahmed clearly articulates his position from slightly different angles than Bowen (2009), however, he similarly warns the reader that the proper performance of document analysis implies certain precautions and quality controls from the researcher:

> In every case [of document review], data must be handled scientifically. Scott (1990) has formulated quality control criteria for handling documentary sources. These are: authenticity, credibility, representativeness and meaning. Authenticity refers to whether the evidence is genuine and from implacable source; credibility refers to whether the evidence is typical of its kind; representativeness refers to whether the documents consulted are representative of the totality of the relevant documents, and meaning refers to whether the evidence is clear and comprehensible. (Ahmed, 2010, p. 3)

The four above-mentioned quality controls for document analysis are actually consonant and consistent with the suggestions made earlier by Bowen (2009). They have been thoroughly implemented and systematically enforced by the researcher as described in the previous paragraph.

Of note, the researcher anticipatorily considered and critically assessed the incorporation of additional research methods, such as surveys and focus groups, to broaden the research and

triangulate the research findings. Nonetheless, after critically pondering the research topic, its context, and the requisite profiles of human subjects for interviewing, it became self-evident that information-gathering methods relying on live interactions and data collection from human subjects would bring little practical value to the research. Among the participants envisaged for the contemplated interviews—professionals from law enforcement agencies, public prosecutors, and criminal defense lawyers—all are bound by strict requirements of professional secrecy, deontology, and ethics that would surely lead to incompletely or selectively answered questions, eventually painting a misleading or otherwise flawed picture. The foregoing drawbacks of interviews and focus groups have been voiced in the past by Wilkinson (1998) and Cheung (2014), corroborating that in research such as this one, interaction with human subjects may rather be counterproductive for the research goals.

§ 3.3 Research Credibility and Peer Debriefing

In view of the previous section, instead of methods triangulation and other conventional ways to enhance research validity and reliability, this dissertation deployed a peer-debriefing technique designed for "filling the role of critic, auditor, detective, and expert observer and listener," as described by Janesick (2015, para. 3). Although peer debriefing is a relatively uncomplicated to perform, it helps significantly enhance the validity and credibility of a qualitative research:

> A good qualitative researcher plans ahead and includes a space for peer debriefing or some variation of it. Peer debriefing allows a qualified peer researcher to review and assess transcripts, emerging and final categories from those transcripts, and the final themes or findings of a given study. Also, a peer may review selected site documents, observational notes, and possibly other written work of the researcher. This peer may

> assess whether or not a researcher has missed a key point, overemphasized a minor one, or repeated one or more points. In addition, a peer acts as a sort of critical detective and is similar to an auditor auditing the ledgers of finance. Many writers have suggested that peer debriefing enhances the trustworthiness and the credibility of a research project (Lincoln and Guba, 1985; Spall, 1998; Janesick, 2011; Spillett, 2003). (Janesick, 2015, para. 1)

Therefore, this research conducted a three-step peer debriefing process to ensure the validity and credibility of the findings. First, during the planning phase of the research, peers of the researcher, who are briefly described below, were contacted to review the research scope, design, and method. Second, for the literature review process, these peers were requested to scrutinize the list of publications and sources for inclusiveness and impartiality to ascertain that no major publications arguing either for or against lawful hacking were missing. Third, when five chapters of this dissertation were ready, the peers conducted a final review of the overall research structure and its conclusions.

The feedback received from the peer debriefings was aggregated into several specific improvements and enhancements of this dissertation and then duly incorporated into the research body. Peers who participated in one, several, or all of the aforementioned stages of the peer debriefing process included the following: (i) three senior law enforcement officers involved in investigations of serious crime through search and seizure of electronic evidence; (ii) two university professors from the faculties of law; (iii) two university professors from social sciences faculties (criminal justice and politics); (iv) two practicing lawyers with significant experience in criminal defense involving complex disputes over digital evidence admissibility; and (v) three experienced cybersecurity experts actively practicing in the area of digital forensics

and incident response. Seven peers had a doctoral degree, while five other peers had at least a master's degree in the field of their practice. All peers were coming from either North America or Europe.

§ 3.4 Examples of Lawful Hacking Legislation

As mentioned in the first chapter of this dissertation, the document analysis was started in the literature review in the Chapter 2. In this chapter, the researcher will continue the document analysis process but solely focusing on examples of lawful hacking legislation enacted at the time of writing. The most recent systematic compilation of national legislation on lawful hacking produced by, or under direction of, a governmental body was over five years old at the time of writing (Gutheil et al., 2017). Therefore, a new research and review of the legislation is required. Below, the researcher will explore several representative examples of modern legislation on lawful hacking by police and other law enforcement agencies within criminal investigations. The selection of countries was tailored to include both Civil and common law jurisdictions, as well as to demonstrate certain polarized examples of a comprehensively codified regulation and a total absence thereof. In addition, the selection of the countries purports to include divergent approaches to privacy safeguards, comparing the traditionally privacy-friendly EU legislation with privacy regimes from non-EU countries from the both sides of the Atlantic.

Importantly, this compilation is not intended to be, and should not be construed as, a comparative or historical study of national legislation of lawful hacking by police within criminal investigations. Rather, this section of the dissertation merely illustrates the currently enacted approaches to the regulation of investigatory cyber operations conducted by police in different countries, shedding light on their apparent strengths and weaknesses. Similarly, the legislation review purposely omitted certain common provisions of national legislation present in

all the countries or offering little value to the essence of this research. Likewise, this concise review does not aim to explore any existing or possible conflicts of the statutory or case law on lawful hacking with provisions of constitution, other national legislation, or international law, respectfully leaving this convoluted and complex topic for another study. For the purpose of simplicity, the positive legislation (lex lata) is provided herein without describing historical debates related to its enactment or amendments after the enactment. Analogously, arguments for any changes or amendments of the enacted legislation—adduced both by the opponents and proponents of lawful hacking—are omitted herein, leaving the scholarly discussion of normative law (lex ferenda) beyond the borders of this applied research. The discussed countries below are ordered alphabetically, by name.

§ 3.4.1 France

In France, an EU-member country, lawful hacking by police is permitted and codified, allowing law enforcement officers to deploy the so-called "special investigation techniques" designed to combat against and investigate organized or serious crime by, inter alia, offensive cyber operations to remotely collect digital evidence (European Judicial Network [EJN], 2020; Council of Europe Committee on Counter-Terrorism [CDCT], 2021). The rules for the lawful interception of digital communications and remote hacking by police are provided in the French criminal procedure code (Code de procédure pénale, CPP; version of August 5, 2022) in Articles 706-95 to 706-95-3. Interestingly, the installation of spyware, keyloggers, and other hidden surveillance tools or devices that require physical access to suspects' digital devices or a physical presence of law enforcement agents is separately governed by Articles 706-102-1 to 706-102-5 of the French CPP. Swire et al. (2016) describe French criminal procedure as comparatively complicated, offering a multistage investigatory power "relying on the acts that can be performed

at each stage of the investigation, as well as the investigative authority of a particular actor, such as a public prosecutor or a magistrate" (p. 342).

As elaborated in Article 706-95 of the CPP, for investigations of serious crimes, comprehensively enumerated in Articles 706-73 and 706-73-1, a special tribunal may, upon receipt of a sufficiently detailed request from a public prosecutor justifying the necessity of such measures, grant authorization to intercept or record the telecommunications of suspects for a period not exceeding one month, which may be subsequently renewed for the same period of time. The process must be supervised by the special judge. Articles 706-95-1 and 706-95-2 specifically address lawful hacking by broadly authorizing the remote and secret search of electronic equipment for the digital evidence necessary for criminal investigation or prosecution. As a privacy-protective counterbalance, Article 706-95-3 of the CPP narrows the permitted scope of remote searches. First, the purpose of the search must be restricted to the investigation of a specific crime for which the judicial approval has been obtained, whereas any evidence collected from "fishing expeditions" is expressly declared inadmissible. Second, a supplementary protection and additional approvals are required if the remotely searched electronic device belongs to, or is operated by, lawyers, magistrates, or lawmakers. Notwithstanding the foregoing, if during an authorized search, conducted within the properly designed scope of a cyber investigation, incriminating digital evidence of another crime is found, which was previously unknown to or uninvestigated by the prosecution, this evidence may be admissible in further judicial proceedings.

While Skrypnyk and Titko (2019) note that the "French [CCP] covers the full range of possible cases of obtaining and using digital evidence, with the simultaneous installation of information security guarantees introduced in the Act on Information Technology, Data and Civil

Liberties in 1978" (p. 10), Liguori (2020) judiciously remarks that "even though the [CPP] framework is reasonably thorough, there seems to be no legal device concerning transparency and accountability of lawful hacking activities, vulnerabilities, or impacted individuals" (p. 25). In sum, the French approach to lawful hacking provides a concise, albeit equivocal and broad, regulation of relation cyber operations conducted by national law enforcement agencies within criminal investigations. Resultingly, French legislation may be prone to an inconsistent interpretation and subsequently flawed execution of cyber operations by law enforcement agents, diminishing the predictability and consistency of criminal justice processes that rely on remote searches of electronic devices.

§ 3.4.2 Germany

In Germany, another EU member state, lawful hacking is also authorized and codified by national legislation. However, compared to France, the German statutory law provides more operational guidance and technical details, paying quite some attention to the technical aspects and nuances of cyber operations. German law also offers significantly more rights and protection to the suspects subjected to lawful hacking operations. On the federal level, cyber operations by police are governed by the German Code of Criminal Procedure (Strafprozeßordnung; StPO version of July 11, 2019) and by the Federal Criminal Police Office Act (Bundeskriminalamtgesetz, BKAG), creating a slightly more complicated and multidimensional legal structure compared to other Civil law countries (Skorvanek et al., 2019).

Remarkably, in vivid contrast with most other jurisdictions, Germany's constitution confers its citizens a unique protection of confidentiality and integrity of electronic devices from unlawful interference, making it a separate and standalone constitutional right (Abel & Schafer, 2009; Momsen, 2022). As a consequence, lawful hacking in Germany is procedurally segregated

from lawful interception and other, theoretically less-intrusive, capacities designed to facilitate criminal investigations. Cyber operations conducted by police detectives likewise require additional precautions and justifications, explaining the utmost necessity of such an operation to be annunciated by a public prosecutor when seeking a court warrant. Furthermore, to protect the privacy of suspects and innocent third parties, police spyware cannot be used, for example, to covertly capture live sound or video stream from device's microphone and camera unless absolutely and specifically required for the investigation (Lindemann & van Toor, 2018).

Lawful hacking is minutely elaborated in Section 100b ("Covert remote search of information technology systems") of the StPO. The section states that "technical means may be used even without the knowledge of the person concerned to gain covert access to an information technology system used by the person concerned and to extract data from that system" (StPO, 2019, Section 101b, para. 1). Notwithstanding the foregoing, the text of the StPO then imposes strict conditions and limitations for when lawful hacking techniques can be leveraged by German law enforcement agencies. Firstly, lawful hacking may solely be applied within the investigations of particularly serious crimes, which are exhaustively defined in the code. Secondly, the nature and circumstances of the investigated offense must likewise be particularly serious, regardless of the formal classification of the underlying offense. Thirdly, lawful hacking is permitted only as a last resort, when all less intrusive means of police investigation were, or would be, largely inefficient and futile. The exhaustive list of the particularly serious crimes is produced in the second paragraph of Section 100b. Finally, under provisions of the third paragraph, only the suspect itself may be the target of lawful hacking, however, third-party systems may also be affected by a police cyber operation, as minimally as is possible, if doing so is reasonably unavoidable and indispensable to the eventual success of the investigation.

Consistent with the foregoing operational restraints, the technical means and methodologies of lawful hacking are also narrowed down to the bare minimum, offering almost paranoid precautions to preclude unnecessary interference with suspects' rights and freedoms guaranteed by the constitution. For instance, police officers in charge of remote searches shall pay particular attention to the integrity and safety of remote equipment, making "only those changes […] to [the target] system which are essential in order to capture the data; and [ensuring that the changes are] automatically reversed once the measure is concluded, insofar as this is technically possible" (StPO, Section 100a, para. 5). Furthermore, the entire process of lawful hacking and the subsequent storage of seized evidence shall not endanger the security of the suspect's devices or information extracted therefrom: "the [technical] means used shall provide protection against unauthorised access using methods reflecting the state of the art. Copied data shall be protected against modification, unauthorised deletion and authorised inspection using methods reflecting the state of the art" (StPO, Section 100a, para. 5). The foregoing provision also establishes a reliable process for safeguarding the integrity and authenticity of electronic evidence collected by lawful hacking in compliance with the scientifically backed chain-of-custody requirements. On top of this, all hacking activities must be painstakingly protocoled and made available for inspection, including:

> (1) the designation of the technical means and the time of their use, (2) information required to identify the information technology system and changes made, which are not only transient, (3) information enabling the identification of the data captured, and (4) the unit implementing the measure. (StPO, Section 100a, para. 6)

Unsurprisingly, an extra layer of strong protection for the private life of a suspect is also expressly incorporated into the German law:

> Where possible in the case of measures under section 100b, technical means shall be employed to ensure that data concerning the core area of the private conduct of life are not captured. Findings made on the basis of measures under section 100b which concern the core area of the private conduct of life shall be deleted without delay or submitted to the court ordering the measure by the public prosecution office for a decision as to their usability and deletion. The court's decision concerning the usability of the data shall be binding in respect of the further proceedings (StPO, Section 100d, para. 3).

The procedural requirements and precautions, necessary to obtain a search warrant for police hacking, are elaborated in the second paragraph of the StPO Section 100e. They may appear even stricter and somewhat unnecessarily burdensome for prosecution: only a mid-level regional court may authorize a lawful hacking operation upon request from a public prosecutor. In case of emergency, a presiding judge may alone issue an order to proceed, however, the order must subsequently be ratified by the competent court within the next three days, otherwise it becomes null and void. The duration of a cyber operation cannot exceed one month. However, it can be successively renewed, whereas if the cumulative duration of operation exceeds six months, a higher regional court gets the exclusive competence for subsequent renewals. Furthermore, a public prosecutor must, inter alia, expressly and minutely specify in its request to the court "as precise a designation as possible of the information technology system from which data are to be captured" and justify "the essential considerations concerning the necessity and proportionality of the measure" (StPO, Section 100e, paras. 3-4). Ultimately, the suspect and all significantly affected third parties, whose devices were searched or otherwise impacted by cyber detectives, must be notified about the executed lawful hacking activities "as soon as it can be

effected without endangering the purpose of the investigation" (StPO, Section 101, para. 5), subject to some narrow exceptions that must be unconditionally approved by court.

Finally, prosecutorial reports about all lawful hacking operations must be provided on an annual basis by the Federal Public Prosecutor General to the Federal Office of Justice. The latter is responsible for preparing a summary—to be openly published on the internet—as stipulated by Section 101b of the StPO. In conclusion, the German approach to lawful hacking is, arguably, the most favorable for the suspect and the most cumbersome for law enforcement agencies, setting a wide range of solid precautions and safeguards that may possibly appear superfluous.

§ 3.4.3 Netherlands

In the Netherlands, the third EU state concisely reviewed in the chapter, lawful hacking by police within criminal investigations is comprehensively regulated by the Computer Crime III Act (Wet Computercriminaliteit III), which amended the Dutch Criminal Code (DCC) and the Dutch Code of Criminal Procedure (DCCP), among other things, to empower the law enforcement agencies to conduct offensive operations in cyberspace when investigating serious crimes (Pool & Custers, 2017; Skorvanek et al., 2019). Under the DCCP (version of July 1, 2022), lawful hacking activities permitted to be conducted by police are carefully sliced into five distinct categories: (i) identification or deanonymization of a person or localization of a digital device; (ii) interception and recording of oral or written electronic communications; (iii) continuous monitoring of a suspect's activities; (iv) search and seizure of digital evidence; (v) and, remarkably, deletion of illicit materials (DCCP, Art. 126nba, para. 1). The foregoing investigatory powers are generally limited to the suspect and its personal digital devices, however, third-party electronic equipment, which is regularly used or shared with the suspect,

may also be compromised by cyber detectives within investigations when it is indispensable for the ultimate success of the operation (Skorvanek et al., 2019).

As in to other jurisdictions, deployment of lawful hacking operations in the Netherlands is restricted to serious crime investigations and only if less intrusive alternatives are unavailable. In addition to those common prerequisites, under the Dutch law, a hacking operation must also be urgently required for an ongoing investigation, raising the bar of necessity higher than it is in other countries (Moraes, 2020). Procedurally, and also somewhat idiosyncratically, permitted technical modes of hacking in the Netherlands are bifurcated by the severity of the investigated offense. Serious crimes, namely those that require a pretrial detention of the suspect for safety reasons and being punishable at least by four years of imprisonment, allow for the interception of live communications, including voice, video, and typing; by contrast, only particularly serious crimes—punishable by at least eight years of imprisonment—enable police officers to stealthily break into remote electronic devices to seize already existing digital evidence or to continually monitor for new incriminating materials that may be created and captured in the future (Kortmann, 2020; DCCP, Art. 126nba, para. 1). The second category of the serious offenses also empowers police officers to remotely delete illicit data, such as child pornography, when necessary to, inter alia, prevent its further proliferation (DCCP, Art. 126nba, para. 1e).

To ensure holistic judicial oversight, all cyber investigations conducted by Dutch police under provision of the DCCP must be approved by court. After reviewing a detailed request by a public prosecutor, which shall describe the cyber operation in sufficient detail and justify the necessity of lawful hacking under the circumstances, the court may issue a warrant valid for up to four weeks, renewable for the same period of time on a continuous basis (DCCP, Art. 126nba, paras. 2-3). For emergencies, court approval remains mandatory, however, it may be provided

orally and must be subsequently validated in writing within the next three days (DCCP, Art. 126nba, para. 5). As an extra precaution, the technical execution of cyber operations by police is monitored by the Public Order and Safety Inspectorate (Moraes, 2020).

Once a cyber operation is complete, the public prosecutor in charge must provide a notice to the suspect, as well as to tangentially impacted third parties, about the investigation and performed acts—as soon as possible but without detriment to the investigation or legitimate interests of justice (DCCP, Art. 126bb). Concerned third parties must keep the information about the operation confidential. Additionally, upon completion of a cyber operation, all spyware and other hacking tools must be safely removed from the remote electronic devices without delay: if, for any reason, the removal is technically impossible, operators of the concerned devices shall be informed and provided with some assistance to clean up the system (DCCP, Art. 126nba, para. 6). To ensure the integrity and authenticity of the digital evidence, and to secure the possibility of its subsequent examination by independent forensic experts at the demand of the suspect, police officers in charge of lawful hacking are procedurally obliged to rigorously protocol their activities and preserve digital evidence in conformity with the chain of custody requirements (DCCP, Art. 126ee).

Another interesting and peculiar detail of the DCCP is that it expressly regulates the disclosure of zero-day vulnerabilities. Under the provision of Article 126ffa, vendors must be informed about zero-day flaws exploited by police within lawful hacking operations, unless there is a prevailing investigatory interest to delay notification, subject to the court's approval. In sum, Dutch legislation provides an interesting and unusually comprehensive approach to certain aspects of lawful hacking, creating a visible contrast with other jurisdictions. Its overall construction may, however, appear a little bit complicated, given that some technical and

operational details of lawful hacking are not elaborated in the DCCP directly, being defined in other national laws or supplements thereto (Kortmann, 2020).

§ 3.4.5 Switzerland

Located in the very heart of Europe, Switzerland is a non-EU country well-known for its venerated neutrality. Its statutory regulation of lawful hacking within criminal investigations provides a remarkable example of a clearly and consistently structured legislation, written in an unambiguous and sufficiently detailed manner. The Criminal Procedure Code (CrimPC) of 2007 (status as of July 1, 2022) elaborates the process in Title 5, Chapter 8 ("Covert Surveillance Measures"). The Chapter starts with Article 269 ("Requirements") that specifies fairly strict, but perfectly reasonable, conditions where lawful hacking and other types of covert investigations or surveillances are permissible within criminal investigations:

> The public prosecutor may arrange for post and telecommunications to be monitored if: (a) there is a strong suspicion that an offence listed in paragraph 2 has been committed; (b) the seriousness of the offence justifies surveillance; and (c) investigative activities carried out so far have been unsuccessful or the enquiries would otherwise have no prospect of success or be made unreasonably complicated. (CrimPC, 2022, Art. 269, para. 1)

The second paragraph of Article 269 provides an inclusive list of serious, or otherwise important as a matter of public policy, crimes that may justify the deployment of covert investigations by police, including lawful hacking operations in cyberspace. Unambiguously alluding to the problem of encryption that undermines efficiency of traditional lawful interception, Article 269ter ("Use of special software for the surveillance of telecommunications") transparently stipulates when lawful hacking can be performed:

> The public prosecutor may order the introduction of special software into a data processing system in order to intercept and recover the content of communications and telecommunications metadata in unencrypted form provided: (a) the conditions of Article 269 paragraphs 1 and 3 are met; (b) the proceedings relate to an offence listed in Article 286 paragraph 2; (c) previous telecommunications surveillance measures under Article 269 have been unsuccessful or surveillance with these measures would be futile or disproportionately difficult. (CrimPC, 2022, Art. 269ter, para. 1)

Next, the second paragraph of the article also requires that the public prosecutor expressly specify and describe the data that is required to be captured by cyber investigators, setting perimetral borders to prevent a blanket or unselective extraction of information from suspect's devices. Importantly, the third paragraph mandates that "data not covered by paragraph that is collected when using such software must be destroyed immediately" and expressly prohibits the use of collected data unrelated to the investigation: "no use may be made of information obtained from such data" (CrimPC, 2022, Art. 269ter, para. 3). Finally, paragraph four of the article imposes a responsibility upon the public prosecutor to maintain a record of lawful hacking operations conducted under its supervision.

Technical precautions and safeguards in relation to the reliable preservation and unalterable authentication of electronic evidence when deploying police spyware are concisely but clearly enumerated by Article 269^{quater} ("Requirements applicable to special software for the surveillance of telecommunications"):

1. The only special software that may be used is that which records the surveillance unalterably and without interruption. The record forms part of the case files.

2. The recovery of data from the data processing system under surveillance to the relevant criminal justice authority must take place securely.
3. The criminal justice authority shall ensure that the source code can be checked in order to verify that the software has only legally permitted functions. (CrimPC, 2022, Art. 269^{quater}, paras. 1-3)

Further, Article 270 authorizes the usage of lawful hacking against the suspects (referred as the "accused") and also against third parties when "there is reason to believe based on specific information that: (1) the accused uses the postal address or the telecommunications service of the third party, or (2) the third party receives certain communications on behalf of the accused or passes on communications from the accused to another person" (CrimPC, 2022, Art. 270). In continuation, a strong protection of regulated professions—including but not limited to public officials, journalists, and "members of the clergy, lawyers, defence lawyers, notaries, patent attorneys, doctors, dentists, pharmacists, psychologists and assistants to such persons" (CrimPC, 2022, Art. 171)—is likewise lucidly prescribed by the law:

> When monitoring a person belonging to one of the professions mentioned in Articles 170–173, the court must ensure that information that is relevant to the enquiries or the reason why this person is being monitored is separated from information that is relevant, in order to guarantee that no professional secrets come to the knowledge of the criminal justice authority. The separated data must be destroyed immediately; it may not be evaluated. (CrimPC, 2022, Art. 271, para. 1)

Procedurally, any and all lawful hacking operations ordered by a public prosecutor must be duly authorized by a special court (referred as the "compulsory measures court") as imposed by Article 272 of the CrimPC. A public prosecutor must submit a plea to the court within 24 hours

of ordering surveillance by lawful hacking, comprehensively detailing the scope and reasons why such intrusive measures are required for the investigation. The court shall grant or refuse the authorization within the following five days: when the operation is authorized, the court shall indicate "(a) which measures must be taken to protect professional confidentiality; (b) whether non-public spaces may be entered in order to introduce special software into the relevant data processing system" (CrimPC, 2022, Art. 274, para. 4). Notably, the duration of a cyber operation is capped by a three-month limit, after which the authorization must be renewed by the court prior to its expiration. If the judicial authorization is refused, the hacking operation must be immediately halted. The usage of electronic evidence obtained from cyber operations that did not receive court approval is flatly prohibited by Article 277 ("Use of the results of unauthorised surveillance operations"):

1. Documents and data carriers obtained in unauthorised surveillance activities must be destroyed immediately. Postal items must be delivered to the addressee immediately.
2. The results of unauthorised surveillance operations may not be used. (CrimPC, 2022, Art. 277, paras. 1-2)

Evidencing a well-thought-out and properly balanced approach to lawful hacking in Switzerland, digital evidence, that is obtained during an authorized lawful hacking operation and exposing previously unknown crimes committed by the suspect or by third parties, may be utilized by the prosecution condition to "these findings may be used against the accused provided surveillance would have been permitted in the investigation of the offences concerned" (CrimPC, 2022, Art. 278, para. 1). Interestingly, considerably broader leeway is left for intelligence gathering: "any findings made in a surveillance operation may be used to trace wanted persons" (CrimPC, 2022, Art. 278, para. 5), again illustrating a carefully calibrated equilibrium of the suspect's and law

enforcement's rights and interests. Finally, the notification to the suspect and other concerned parties, as well as exceptions thereto, are prescribed in a detail by Article 279 ("Notice"):

> The public prosecutor shall notify the suspect under surveillance and third parties under surveillance in terms of Article 270 letter b of the reason for and form and duration of the surveillance operation on conclusion of the preliminary proceedings at the latest. (CrimPC, 2022, Art. 279, para. 1)

Clearly defined and unequivocal exceptions to the notification requirements do exist and likewise incorporate a fair and reasonable balance of individual rights and the interests of the criminal justice system:

> With the consent of the compulsory measures court, notice may be deferred or dispensed with if: (a) the findings are not used as evidence in court proceedings; and (b) deferring or dispensing with notice is necessary to protect overriding public or private interests. (CrimPC, 2022, Art. 279, para. 2)

In conclusion, Swiss legislation provides a laudable example of a simple, clear, and comprehensive regulation of lawful hacking by police within the investigation of serious and organized crime. The rights of the suspect are sufficiently and predictably protected, whilst the legitimate needs of law enforcement agencies are not regarded through the prism of supreme and overshadowing privacy protection (as, e.g., in the German law discussed above). Importantly, the legislation is structured and transcribed in a lucid language, being unencumbered with legalese, jurisdiction-specific terms, or excessive cross referencing.

§ 3.4.6 United Kingdom

The United Kingdom is the only European country with a common law system, being one of the oldest jurisdictions, with a fascinating history of case law and judge-made legal doctrines.

Since the United Kingdom is no longer a part of the EU, it must adopt its national legislation to the new context and novel realities, enjoying less restraints than were previously imposed by the pressing stack of EU laws. Under the U.K. law, lawful hacking by law enforcement agencies within criminal investigations is softly labeled as "equipment interference," being thoroughly regulated and codified by Part 5 ("Equipment Interference") of the Investigatory Powers Act (IPA) of 2016 (Gutheil et al., 2017). The full text of the Act is set forth on as many as 305 pages without counting numerous supplements, for instance the Equipment Interference Code of Practice of 2018: another impressive document spanning on 147 pages, evidencing the relevant complexity and even comparative cumbrousness of the British regulation of lawful hacking. This observation is, however, not made to criticize the U.K.'s approach: utmost care and attention were given by legislators to almost to every legal and operational detail of the regulation, so it represents an interesting example for other countries.

Whilst all cyber operations conducted by police require a warrant, as mandated by Section 106(1)(a) of the IPA, the warrant may be issued both to prevent and to investigate crime, granting British law enforcement agencies a fairly extensive and invasive power to conduct proactive operations in cyberspace (Brown, 2020). Following the provisions of Sections 106(1) and 109 of the Act, a warrant can be issued by a law enforcement chief and then approved by a Judicial Commissioner, unless there is an emergency that would allow the law enforcement chief to retroactively approve the warrant within the next three days. In continuation, telecommunication providers are obliged to assist—within reason and when technically feasible—in the implementation and execution of lawful hacking warrants as mandated by Section 128 of the Act. Additionally, lawful hacking operations can be deployed to obtain both digital communications and stored electronic data, broadly and inclusively defined in Sections

100, 101, and 135 of the IPA, providing law enforcement agencies with a *carte blanche* to extract virtually any type of data or communications from remote systems (Skorvanek et al., 2019). Another strikingly unique, albeit understandable, particularity of the Act is that equipment interference is expressly permitted against electronic devices located in foreign jurisdictions when the suspect is a U.K. national or if the investigated crime has a direct connection to the U.K. judicial system (Davies, 2020). Whether such unusually broad but necessary power may verge on violation of international law is not yet clear. The legality of extraterritorial operations is discussed in the next sections of this chapter.

Noticeably, to reassure British residents that lawful hacking will not be arbitrary or inadmissibly overbroad, the IPA also contains a considerable number of privacy-protection precautions and requirements. Firstly, lawful hacking can be solely deployed for the investigation or prevention of a crime punishable by a prison sentence of three or more years, as defined by Section 263 of the Act. Moreover, a cyber operation has to be necessary for the investigation and proportional under the totality of circumstances as per Section 106(1) of the IPA. Secondly, Sections 111 to 114 and 131 of the Act establish supplementary requirements and extra protections when lawful hacking implicates lawmakers, journalists, lawyers, or any privileged communications thereof. Thirdly, whilst being in a visible discrepancy with other jurisdictions, the duration of a warrant must not exceed six months, as directed by Section 116 of the IPA, subject to succeeding renewals (Davies, 2020). Fourthly, Section 129 elaborates technical and operational precautions related to the storage, processing, and retention of seized digital evidence, ensuring that the data will be duly protected from unauthorized access and will not be retained longer than necessary. Procedurally, the Act has also created a dedicated oversight body—the Investigatory Powers Commissioner (IPC). Additionally, the IPA granted

supplementary powers to the Investigatory Powers Tribunal (IPT) to hear complaints from aggrieved persons about excessive or otherwise abusive equipment interference, such as alleged violations of the privacy-protection provisions of the Human Rights Act (HRA) of 1998 (Trummer, 2020). Finally, even more operational and technical details on the foregoing mandatory precautions are thoroughly elaborated in Sections 8 to 10 of the Equipment Interference Code of Practice.

Reportedly, alongside the United States, the United Kingdom globally leads lawful hacking operations by law enforcement agencies within criminal investigations, orchestrating highly creative and innovative cyber operations with, for instance, the deployment of advanced mobile spyware and painstakingly planned cyberattacks targeting dangerous criminals in a smart and efficient manner (Gutheil et al., 2017; Keenan, 2019). Being a part of the U.K.'s statutory law, the IPA's overly detailed, long, and scrupulously written text is somewhat expectable, making it a fairly complicated piece of legislation. However, the Act certainly serves as a rich source of valuable knowledge and practical considerations for other countries that have no statutory law to regulate lawful hacking. In the wake of the Brexit, additional regulatory changes in relation to lawful hacking are foreseeable in the United Kingdom, probably providing the British government with supplementary policing powers to prevent and prosecute serious and organized crime in the British Kingdom.

§ 3.4.7 United States

In stark contrast to all countries discussed above, the United States has no statutory legislation that expressly authorizes or prohibits lawful hacking activities by police within criminal investigations. In parallel, U.S. federal law enforcement agencies—as illustrated by numerous examples adduced in Chapter 2—have been pioneering offensive cyber operations to

investigate and prosecute serious crimes within its own borders and internationally (Brown, 2020). Unsurprisingly, large-scale hacking operations in cyberspace, uncorroborated by a statutory law, fuel polemics and create a peculiar legal paradox that do not, however, prevent the efficiency of those operations (Liguori, 2020). Procedurally, in the United States, a valid search warrant from a judge is required to lawfully extract electronic evidence from a remote electronic system without violating, inter alia, the Fourth Amendment of the U.S. Constitution, which protects American residents from unreasonable searches and seizures (Skorvanek et al., 2019). This legal safeguard was, of course, not designed or even foreseen for lawful hacking, being currently operationalized in a form of extrapolation as the most relevant piece of legislation.

In 2016, the Federal Rules of Criminal Procedure (FRCP) were updated to address the multiplying attempts—undertaken by inventive defendants in criminal cases—to challenge the validity of search warrants issued for lawful hacking investigations. Prior to 2016, the FBI and other federal agencies were successfully leveraging lawful hacking techniques to unmask criminals who were trying to conceal their true identity and device location, using various widespread anonymization technologies such as TOR or VPN (Russell, 2017). Eventually, during court trials, the uncovered and subsequently arrested criminals vehemently disputed the legal validity of the search warrants, asserting that the issuing court had no territorial jurisdiction over their computer. They subsequently demanded suppression of the digital evidence collected pursuant to the warrant. Under the updated version of the FRCP, a federal judge is empowered to "to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if […] the district where the media or information is located has been concealed through technological means" (FRCP, Rule 41(b)(6)). This FRCP amendment provides fairly broad investigatory power to law

enforcement agencies when wrongdoers exploit anonymizing technologies to evade police radars (Mayer, 2018; Skorvanek et al., 2019). Importantly, when the physical location of electronic evidence is known, the warrant must be issued only by the court having territorial jurisdiction over the venue; otherwise, the electronic evidence collected under the warrant will likely be inadmissible in court.

Consonantly with the recent case law and the prevailing opinion that remote hacking and usage of spyware to obtain incriminating digital evidence within criminal investigations is legal—or at least not illegal—in the United States, Welty (2018) agrees that those techniques are generally permitted and lawful when executed properly. He notes that to avoid problems with the admissibility of digital evidence in court proceedings, search warrants should be carefully and precisely drafted, namely ensuring that the issuing court has territorial jurisdiction over the evidence, as well as that the operation is not overbroad or disproportionally intrusive. Mayer (2018) likewise mentions that when requesting a search warrant, police officers should convincingly demonstrate a probable cause that the remote search will bring particular evidence of a specific crime. This requirement is often not an easy task within digital investigations: the sought evidence may be stored on an unidentified device in an unknown location, be fragmentedly dispersed over several devices simultaneously, or have an unpredictable size and format. Mayer also reminds that it is important to consider prudently the perimeter and temporal duration of a search warrant for multistage hacking operations. For instance, police officers are to evaluate whether the ongoing backdooring of a website's visitors, accomplished through an already compromised and backdoored web server under a warrant, would require an extension of the warrant's duration and scope, as it may constitute an ongoing search operation if the electronic evidence is continually exfiltrated from the compromised devices of the website

visitors. Mayer ultimately also questions whether, when, and how the government must provide notice to the owners of compromised electronic devices under the relevant FRCP provisions. Other scholars suggest that the statutory legal vacuum, in relation to lawful hacking in the United States, does not dispense U.S. law enforcement agencies from their duty to notify persons searched under a warrant, including remote cyber searches, following the requirement of Rule 41(f)(1)(c) of the FRCP (Osula & Zoetekouw, 2017).

In continuation, Mayer (2018) adduces some though-provoking examples of currently unsettled legal questions (e.g., whether a super-warrant doctrine is applicable for lawful hacking). He calls for a better regulation and codification of rules in relation to search and seizure in cyber operations to avoid the protracted uncertainty. In sum, a codification of lawful hacking by police would provide undisputable advantages both to law enforcement agencies and to society by increasing the predictability and certainty of cyber operations against organized and serious crime, whilst offering significantly more clarity in relation to privacy protection.

§ 3.5 Extraterritoriality and Tallinn Manual

Arguably, the most uncertain and delicate, through essential, element of legislation on lawful hacking regards extraterritorial cyber operations that may require, for example, access to digital devices, equipment, or data stored in a foreign sovereign state. Cyber investigations, as discussed in this dissertation, are performed by competent governmental authorities and, therefore, are attributable to the conducting state. If such cyber operations cross the state borders and cause a palpable effect abroad, specifically without authorization or without another legal basis available under international law, the operations may, among other things, infringe sovereignty of the foreign state and potentially constitute an internationally wrongful act. Whilst

this dissertation does not purport to assess the legality of cross-border cyber operations through the prism of international law, it is nonetheless important to discuss the topic in this chapter.

The researcher believes that one of the best sources of international cyber law is the second edition of Tallinn Manual, known as "Tallinn Manual 2.0." The 598-page manual was prepared by a group of international experts at the invitation of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Center of Excellence (CCDCOE). The Director and General Editor of the Manual is Professor Michael Schmitt, one of the most venerated experts and legal scholars in the area of international cyber law. To set a general foundation for the territorial jurisdiction of lawful hacking, Rule 9 of the Manual may be helpful:

> A state may exercise territorial jurisdiction over: (a) cyber infrastructure and persons engaged in cyber activities on its territory; (b) cyber activities originating in, or completed on, its territory; or (c) cyber activities having a substantial effect in its territory. (Schmitt, 2017, p. 55)

The letter (a) of the Rule crystalizes the authority of a state to engage in cyber operations on its own territory if this does not violate other duties owed under international law, for instance, the inviolability and protection of the foreign diplomatic and consular cyber infrastructure located on that state's domestic soil, which are comprehensively covered by Rules 39 to 44 of the Manual. The foggiest realm of legal uncertainly is created by cyber operations that cross national borders and target foreign citizens, infrastructure, or data located abroad. The partial answer about the legality of such operations under international law can be found in letters (b) and (c) of the Rule 9. The researcher believes that the following key factors are to be considered when legislating on cyber operations that may create an impact abroad: (i) the legitimate interest of the foreign state to exercise its jurisdiction over the investigated crime that may fall into the *domaine*

réservé of the foreign state; (ii) the scale and nature the cyber operation's impact on the infrastructure, data, or people located abroad; and (iii) duties that the conducting state may owe under the international law when conducting operations in cyberspace, for instance, duties imposed by MLATs or international conventions. The more interest a foreign state may reasonably have in prosecuting the crime in question, the greater the chances that a cyber operation, targeting digital evidence requisite to solve a crime on the foreign soil, may amount to an internationally wrongful act. Likewise, the more perceptible, material, and tangible impact happens on the foreign soil as a result of cyber operation: for example, massive data corruption or the outage of a foreign data center boosts the likelihood that the cyber operation will constitute a wrongful act under international law unless expressly authorized by the foreign state. The wrongfulness may potentially be precluded by certain circumstances, but few of them apply for lawful hacking operations aiming at the cyber investigation of serious or organized crime abroad.

Remarkably, it seems that British legislators, as discussed in a previous section of this chapter, considered the foregoing elements and granted a carefully worded authority to conduct cross-border cyber operations to its national law enforcement agencies. Whilst at the time of writing those provisions have not been tested for the legality under international law, they seem to be reasonably adopted to the contemporary needs and realities of international law in cyberspace. In conclusion, lawmakers should consider naming an expert commission to ensure that their national legislation on lawful hacking will not infringe international law. Tallinn Manual 2.0 may be a perfect place to start their research and analysis.

§ 3.6 Greater Good Concept

In the absolute sense, none of the six national regulations of lawful hacking, as reviewed in the previous sections of this chapter, overarchingly address the growing plurality of legal

problems and technical challenges discussed in Chapter 2. Whilst national legislation on lawful hacking in some jurisdictions offers conspicuous advantages, such as clarity or simplicity, they still have a non-negligible potential to improve both procedural and substantive law, so as to keep pace with technological progress and the ongoing evolution of values within democratic society. The foundational and philosophical principles of lawful hacking legislation are briefly elaborated and discussed below without yet delving into the technicalities and specific legal complexities, leaving this captivating discussion for the next chapter.

The dogmatic concept of a "greater good," conceptualized and operationalized by Brown (2020) within the particular context of lawful hacking, is a perfect prism for both the exploratory and explanatory observation and analysis of national legislation on lawful hacking by police within criminal investigations. To put it differently, the concept of the "greater good" can be semantically reversed to that of a "lesser bad" without loss to its inner meaning or rationality. From the viewpoint of legal philosophy, national legislation on lawful hacking—be it an impeccably codified statutory law or a convoluted set of case law intermingled with judge-made rules—should impartially and fairly balance the interests of society with the rights and freedoms of individuals trapped in the crosshairs of the criminal justice system. The fragile equilibrium should, however, not be mechanically sought in abstraction from the context of investigation, but rather with mindful consideration of the totality of circumstances of each case that may justify intrusive investigations by police in cyberspace.

Penologically and utilitarianly speaking, society has an undeniable and vital interest in preventing, or at least punishing and deterring, serious crime; shielding its law-abiding citizens from deviant behavior; and promoting conscientious social behavior. Whether one accepts or not this as an axiom, one should certainly consider and respect the legitimate rights and freedoms of

suspects, who deserve equal protection under the law despite their condemnable acts. Likewise, a presumption of innocence should be promoted and safeguarded. Moreover, avoidance of excessive or unnecessary intrusive tactics of criminal investigations conducted in cyberspace is equally desirable and beneficial for society: a draconian regime or dictatorial cyber policing will unlikely enhance the sustainable development of a country, neither economically nor socially. Importantly, overbroad cyber operations may be also at odds with international law, creating political and diplomatic tensions with a palpable effect on the national economy. Arbitrary or bulk investigations by police in cyberspace, causing a collateral damage or pervasive feeling of Big Brothering, will certainly boomerang to the ardently overregulating state and irreparably erode citizens' trust and confidence in the government, criminal justice system, and law enforcement agencies.

Yet granting an overarching or unconditional privacy protection to suspects and coddling seasoned criminals will predicably fuel the exponential proliferation of serious and organized crime, bolster the "grey-mailing" phenomenon discussed above, and proliferate other chimeric creatures of impunity inspired by a toothless state. Worse still, at the time of writing, transnational criminal cartels already possess formidable technical and financial resources, largely surpassing the modest operational capacities of law enforcement agencies that prevailingly lack the requisite funding, technical equipment, and human experts to investigate serious crime in cyberspace. The further disarming of police forces is poised to trigger a tectonic shift in society, wherein a golden era of the "perfect crime" will reign amid the incapacitated police and weak government unable to bridle organized crime, perfidiously exploiting the usurped advantages of technical progress to evade justice and further crimes.

In sum, ideally, lawful hacking legislation should provide robust and inviolable protection for the fundamental human rights of suspects and, in parallel, offer a technically efficient and frictionless mechanism by which to investigate and prosecute serious crimes without a bureaucracy, procedural hindrances, or blind overindulgence of privacy. After studying and concisely discussing six national regulations of lawful hacking at the beginning of this chapter, the researcher suggests that an enhanced combination of the Swiss and British approaches, with some minor adjustments and addendums, will derive a sustainable model to regulate lawful hacking in a simple, effective, and equilibrated manner that would be consonant with the foregoing philosophical considerations. Chapter 4 will distill a jurisdiction-neutral and technology-agnostic framework to regulate lawful hacking in a simple but comprehensive manner, considering its interdisciplinary nature.

§ 3.7 Chapter Three Summary

In the beginning of this chapter, the researcher further detailed the selected research method, its suitability, and effectiveness for this specific research and three research questions. Then, carrying on from the document review commenced in Chapter 2 for a better readability and structural consistency of this dissertation, the researcher analyzed and discussed the existing legislation, regulating various aspects of lawful hacking by police within criminal investigations in several common and Civil law countries, to better grasp how countries are currently implementing and enforcing national legislation on lawful hacking. Next, the intersection of national regulation of lawful hacking and international law was briefly discussed. In the end, it was concluded that, based on the legislation review and the issues discussed in the previous chapter, all countries have a considerable space to improve and ameliorate their lawful hacking legislation in one way or another, providing either a better protection of individual privacy or,

contrarily, removing unnecessary barriers that hinder investigations of serious and organized crime.

4. CHAPTER FOUR

§ 4.1 Filling the Gap: Lawful Hacking Framework

Below is a technology-agnostic and jurisdiction-neutral framework designed to provide foundational guidelines for the legislative, judicial, and executive branches of government in the implementation, amelioration, or interpretation of their national legislation on lawful hacking. The present framework may also be helpful for criminal defense lawyers and senior law enforcement officers to better grasp the multidisciplinary intersection of technology and law within cyber operations. The underlying purpose of this framework is to equip the audience with an interdisciplinary knowledge and foundational understanding of the interrelated technical, operational, and legal aspects of lawful hacking to make well-informed and better decisions. Emphatically, the framework has not been adjusted for any specific country, legal system, or jurisdiction, and thus can be leveraged both in common and Civil law jurisdictions. The eventual implementation of framework provisions into a national law on lawful hacking can take various interrelated forms, spanning from the conventional parliamentary lawmaking, when major changes to national legislation are required, to a simple administrative rulemaking by competent national agencies, when so is permitted for minor operational or implementational details requiring updates and improvements.

The framework comprises 15 successive sections, wherein each section concisely discusses a specific set of considerations for national legislation on lawful hacking and proposed ways to address those considerations sustainably for both the law enforcement and society. The sections are not ordered by their technical or legal significance: rather, they are structured in a logical, coherent, and easily readable manner. The framework sections should not be regarded as

isolated legal and technical components, but as a compounded system composed of closely interconnected and interdependent components of the lawful hacking apparatus.

§ 4.2 Lawful Hacking Framework

§ 4.2.1 Authority

A well-thought-out and crystal-clear authority to conduct cyber operations within criminal investigations shall be expressly granted by national legislation on lawful hacking to a limited number of law enforcement agencies, ideally, to a single agency. Sharing the authority to conduct cyber operations among several national agencies—especially when mixing federal, state or provincial, and municipal level agencies—will open the floodgates to unhealthy inter-agency competition, turf battles, and hardly preventable feuds among agencies. Moreover, the centralization of technical competences, such as the development of hacking tools and spyware, will significantly reduce the costs, accelerate the speed, and bolster the overall effectiveness of cyber investigations. Furthermore, the centralization will minimize the impact of smoke-screen operations by cybercriminals and foreign state actors aiming at framing random law enforcement agencies and casting them as the authors of illicit hacking attacks, as elaborated in Chapter 2. With the recognition that the organization of law enforcement powers in each country is unique, stemming from its cultural, historical, and political values, certain universal principles to organize lawful hacking on a national level, which may be efficient and productive for most countries, are discussed below.

First, as will be elaborated in subsequent sections of this framework, lawful hacking shall be restricted to the investigation of only serious and organized crime. Therefore, it will be rational to grant the exclusive authority to perform cyber operations to a single national agency already in charge of the investigation and prosecution of serious crime. In jurisdictions where

several agencies are concurrently empowered to investigate serious crime, the preference should be pragmatically given to the most well-funded agency or to the agency with the longest experience in offensive cyber operations. Exclusivity to perform lawful hacking operations is critical for its sustainability, efficiency, and long-term success. The decentralization of government hacking powers will likely lead to quarrels and conflicts over uncoordinated cyber operations by competing national agencies, redundant investigations exposing confidential hacking operations to suspects, uncertainty and unpredictability over police power and duties, and lesser quality cyber operations executed by smaller agencies with modest budgets and technical expertise. Additionally, if only one national law enforcement agency is officially empowered to conduct lawful hacking, then both judicial oversight and continuous improvement for the entire process, spanning from technical and privacy-protection questions to notifications to all affected parties, will become significantly easier and more agile. Therefore, national legislation on lawful hacking may confer hacking power to one agency and expressly prohibit all other agencies from undertaking, or participating in, any hacking activities—instead requiring them to contact the competent agency when needed. Notably, the competent agency should develop a transparent policy on requesting cyber investigations in a simple manner, as well as implement a 24/7 point of contact to enable other governmental bodies to request a cyber investigation, to the extent permitted by law, and expect that their inquiry will be non-discriminatorily treated with due rigor, speed, and effectiveness.

Second, the national agency in charge of lawful hacking may be empowered to collaborate with national intelligence agencies or special military units, which also conduct cyber operations and related research, but for different purposes than the investigation of serious crime within the country. The sharing of threat intelligence, newly discovered hacking techniques,

special-purpose spyware, and new vulnerabilities or exploits will bring synergy to optimize the costs and boost the efficiency of lawful hacking on domestic soil. Additionally, a well-organized collaboration may even give the central agency (in charge of lawful hacking) access to some sophisticated cybersecurity research conducted by allied foreign states, bringing rocket fuel to the dynamics and efficiency of cyber operations, whilst duly preserving the safeguards imposed by law. The scope and integrity of such collaboration shall, of course, invariably adhere to national lawful hacking legislation, ensuring a consistent and coherent application of law. For instance, if a specific activity within the inter-agency cooperation may preclude or delay the central agency from performing its duties imposed by law, then the risky activity shall be unconditionally avoided. Examples of prohibited activities range from unauthorized sharing of personal data with national intelligence agencies to participation in the development of destructive cyberwarfare that may accidentally inflict uncontrollable damage upon innocent third parties. The full scope of restrictions is detailed in the upcoming sections of this framework.

Third, the national agency running lawful hacking operations may be granted certain administrative rulemaking capabilities to the extent permitted by law. The rulemaking capability will both improve the quality of technical processes or procedures and save the valuable time of lawmakers in parliament. Of course, the permitted rulemaking scope and perimeter are to be unambiguously defined and promulgated in the text of national legislation on lawful hacking. For example, lawmakers may safely delegate to the agency the implementation of administrative procedures related to the due diligence of the agency's employees or the auditing of its internal security controls. Unquestionably, all rulemaking activities shall either be transparently published online or otherwise publicly disclosed so that any interested parties can challenge a specific rule or administrative policy in court, if permitted under national law. Likewise, all rules

shall be subject to an annual audit performed by an independent governmental commission or parliamentary committee to ensure the legality of the implemented processes and procedures.

§ 4.2.2 Jurisdiction

Jurisdiction over foreign-stored evidence, or electronic equipment physically located abroad, is a cornerstone of lawful hacking operations. An imprudent cross-border cyber investigation may infringe upon the sovereignty of a foreign state and could constitute a wrongful act under international law, provoking a domino effect of legal, diplomatic, and political ramifications. International law may also play a pivotal role in purely domestic affairs, for instance, in some jurisdictions, any evidence obtained in violation of international law is inadmissible in national courts. Importantly, national legislation on lawful hacking with an overbroad jurisdiction, visibly neglecting the sovereign interests of other sovereign states or disregarding certain long-established norms of international law, may be perceived by other states as an invitation to reciprocate and conduct offensive cyber operations on the state's territory.

Unsurprisingly, at the time of writing, no state has enacted a *carte blanche* approach to the transborder collection and seizure of electronic evidence. However, the United States and the United Kingdom have made some distinguishable steps in the foggy direction of the legalization of transborder searches under their national law, as discussed in Chapter 3. Countries with a *laissez-faire* approach to cross-border cyber investigations risk being accused of breaking the norms of international law, namely violating the territorial sovereignty of another state, as briefly explained in Chapter 3. In contrast, countries with a wait-and-see strategy flatly prohibiting the seizure of electronic evidence stored abroad are already losing their battle against organized and

serious crime. Legal scholars and state officials have been voicing diametrically opposed views on this controversial and vigorously debated question.

Remarkably, at the time of writing, no international treaty governed lawful hacking specifically, whilst non-intrusive and collaboration-based access to cross-border data is quite comprehensively addressed by the Budapest Convention, as discussed in Chapter 2. This section does not attempt to analyze the eventual legality or wrongfulness of hacking operations by law enforcement agencies aimed to seize electronic evidence located abroad through the multiplex lens of international law. Instead, this section of the framework, in continuation to the relevant provisions of the Tallinn Manual reviewed in Chapter 3, discusses an array of operational and technical implications that may reduce the multispectral repercussions of cross-border searches and seizures of electronic evidence by proactively addressing them via national legislation on lawful hacking.

No state is above the international law. Therefore, among other things, utmost respect should be given to the territorial sovereignty of foreign states. As a rule, relying on the express provisions of bilateral or multilateral MLATs is a safe harbor to lawfully obtain electronic evidence located abroad. Sadly, this legally irreproachable method of interstate collaboration is not always available and is frequently inefficient or even futile, as elaborated in Chapter 2. Nonetheless, accessing foreign-based electronic equipment without express permission from the hosting state does not always amount to a violation of international law. Paradigmatically, among the factors that may potentially reverse the illegality of such access, one should consider the interest of the foreign state in exercising its jurisdiction over criminal offenses happening in a foreign land, as well as digital evidence related thereto. Obviously, the electronic devices of a criminal gang operating and causing impact solely in the foreign state should probably never be

compromised within a cyber operation, unless a valid permission from the foreign is received under an MLAT mechanism or via diplomatic channels. Similarly, if a cyber operation targets a possibly innocent, albeit not totally blameless, third party such as a local operator of anonymous VPN services that are commercialized globally, then express authorization from the operator's home state seems indispensable. By contrast, it is highly unlikely that a country A has a modicum of interest in exercising its jurisdiction over digital evidence related to a crime committed by a citizen of country B and having an effect solely in country B, but stored for a short period of time in a multitenant datacenter in country A by a cloud provider incorporated in country C. Notably, cyber operations that cause palpable material harm or perceptible disruption of foreign infrastructure will likely constitute a violation of international law and should be always avoided. That being said, some exceptions may, but not necessarily will, preclude the wrongfulness of an unwarranted penetration into a foreign IT system or seizure of data stored abroad. These exceptions are briefly discussed below.

First, a justifiable emergency, which can be tentatively labeled a "cyber hot pursuit," for instance, a situation in which there is an imminent risk to person's life or a reasonable certainty that some indispensable digital evidence of a serious crime will be irrecoverably destroyed, may possibly preclude the wrongfulness of unwarranted intervention under the exigent circumstances. In such a case, a post-factum notification may be highly desirable to demonstrate a respect to the foreign state and to preserve a good relationship with it in the future. Going one step further, the state behind a lawful hacking operation that is conducted abroad in emergency may even refrain from using the seized electronic evidence in any judicial or investigatory proceedings before receiving a retroactive "green light" from the foreign state from which the evidence was seized.

Second, if the location of digital evidence is unknown, for instance, due to the "loss of location" phenomenon discussed in Chapter 2, or if it cannot be determined with sufficient certainty, a prudent, non-destructive, and laser-focused cyber intervention may possibly be excusable. For example, if the nationality, domicile, and whereabouts of a dangerous suspect are flatly unknown, it would be a clumsy overkill to seek permission to penetrate into the suspect's devices located in unknown jurisdictions: hypothetically every country in the world would need to be contacted, and most will likely simply ignore such an aberrant demarche. A similar situation may occur when a suspect utilizes advanced anonymizing techniques to conceal its identity or location. In the foregoing examples, it may likewise be advisable to consider a post-factum notification—once the cyber operation is successfully completed—if the whereabouts of the suspect is eventually identified. Moreover, if extradition of the suspect is required, a close collaboration with the foreign state will become indispensable, so it is better to establish a contact at the earliest possible stage of the operation.

Third, if foreign-stored data can be lawfully accessed from a suspect's device already under the licit, albeit secret, control of law enforcement agents, its exfiltration will unlikely amount to an internationally wrongful act. Therefore, the meticulous planning of cyber operations and the assessment of possible implications under international law should always be an integral part of lawful hacking. When planning such operations by police, states should strive to create and promote sustainable partnerships in cyberspace investigations. For instance, if seized digital evidence turns out to be helpful for prosecutorial authorities of a foreign state (e.g., a newly discovered episode of the crime implicating foreign-based victims or perpetrators), the evidence may be shared with the foreign state as a matter comity after completion of the cyber operation.

In conclusion of this section, it is fair to suggest that if relying on MLAT mechanisms does not jeopardize the investigation—it shall be the preferred way of seizing electronic evidence physically located in foreign jurisdictions. In the exceptional cases and narrow circumstances discussed above, a post factum notification or even an annual report reassuring that no foreign-based third parties or governmental systems were impacted in any manner, transmitted via diplomatic channels, may ease the possible erosion of diplomatic relationships and demonstrate due respect to international law. That being said, lawmakers should certainly foresee the convoluted intricacies of international law when legislating on lawful hacking in their home country. The relevant provisions of the Tallinn Manual, briefly discussed in the previous chapter, may be a perfect place to start.

§ 4.2.3 Proportionality

Being an inherently intrusive and distinctively invasive method for conducting criminal investigations, lawful hacking must be legally permitted only in exceptional cases and under exigent circumstances—justifying the use of cyber force by police—when less intrusive means of investigation are unavailable or futile. National legislation without such protections and safeguards, drafted in an unambiguous and textually strict manner, is poised to be ephemeral: in jurisdictions where the judicial branch is empowered to strike down unconstitutional laws enacted by the legislative branch, courts will rapidly terminate the overbroad regulation of lawful hacking. Additionally, violations of different provisions set forth in international conventions designed to shield human rights (e.g., the ECHR discussed in Chapter 2 of this dissertation) may likewise lead to a swift repeal of the unnecessary invasive legislation in ECHR signatory states. Worst, an abrogated law will likely make further efforts to enact a more privacy-friendly version of the law more complicated, contentious, and time-consuming than enacting adequate

legislation on the first attempt. Below are the several principal safeguards in relation to proportionality to bear in mind when drafting national legislation on lawful hacking.

First, the deployment of lawful hacking should be solely authorized to investigate serious crimes, whereas the definition and exhaustive list of such crimes shall be incorporated into the legislation or an annex thereto, to make subsequent amendments—if necessary—less procedurally burdensome. A categorically simple classification of crime seriousness, based on specific articles of the national penal code or just a minimum statutory punishment threshold, may actually do a disservice both to criminal justice and to society. Whilst an exhaustive compilation of criminal offenses—where lawful hacking may be deployed—is essential for transparency, accountability, and predictability of cyber operations, every crime should be regarded through the compounded prism of extenuating and aggravating circumstances. For example, a homicide by excessive use of force in self-defense shall be unquestionably differentiated from a homicide committed within a hate crime. Analogously, a primitive scam, causing just a few dollars of monetary loss to thousands of victims, shall probably not be considered less serious than a sophisticated financial fraud case victimizing one single financial institution for tens of millions. Every criminal offense is unique: the integrity of its circumstances, as well as the legitimate interests of the suspect, victims, and society as a whole, shall be pondered and taken into consideration prior to giving a “green light” to lawful hacking.

Second, lawful hacking should not be used if less intrusive means to attain similar outcomes are available. There is a subtle caveat here: the mere availability of less intrusive means shall not be a decisive factor in isolation from the overall context. Such vital elements of cyber operation as its timing and costs shall be an integral part of the balancing equation. For instance, it would be foundationally unfair to squander thousands of taxpayers’ money or waste

the precious time of law enforcement specialists just to protect the privacy of a dangerous offender. The foregoing does not, however, suggest a purely utilitarian approach to lawful hacking, which would place the financially calculable economic interests of society above intangible human rights. That being said, every criminal investigation is assembled from multiple interconnected ingredients, which should be jointly analyzed and balanced to attain a fair equilibrium for all concerned parties.

Third, necessity is, arguably, the most crucial variable in the proportionality equation. To illustrate this point: when lawful hacking is merely required to obtain some supplementary digital evidence to corroborate an already-solid evidentiary basis that will likely secure a guilty verdict, then even when dealing with the most despicable, heinous, and disgusting felonies, lawful hacking should probably not figure in the prosecutorial arsenal. Contrastingly, for a financial crime of a mid-level gravity that, however, would never be solved without a recourse to lawful hacking, the deployment of cyber detectives may be justified under the general deterrence theory and in view of the prepondering interests of justice. The spirit of the proportionality requirement saturates all other requirements of this framework described below.

§ 4.2.4 Judicial Oversight

To guarantee indiscriminate compliance with the above-mentioned doctrine of proportionality, as well as with other pivotal elements of this framework described below, a mandatory judicial oversight shall be thoroughly implemented for the integrity of lawful hacking operations both in inquisitorial and adversarial legal systems. Selective, or otherwise circumventable, judicial oversight may erode people’s trust and confidence in the judicial system, make the collected electronic evidence inadmissible in a court of law, and stimulate incremental negligence or even misconduct across law enforcement agencies. Finally, a holistic

judicial oversight may shield national legislation on lawful hacking from unavoidable attacks, questioning its legality, in both national and international courts.

Whilst being operationally unrealistic in some jurisdictions, in others, dedicated courts with specially trained judges should be empowered to adjudicate whether and when lawful hacking is permissible. Entrusting this pivotal task to courts of general jurisdiction with technically unexperienced judges is poised to be problematic. Obviously, the creation of standalone tribunals with a unique subject matter jurisdiction over lawful hacking would be overkill, and is certainly not required. Luckily, many jurisdictions already have special courts for complex technical matters or compulsory measures, with specially trained judges whose competences may be naturally expanded to handle all questions of lawful hacking within criminal investigations. The special training, likewise, does not imply judges with doctoral degrees in cybersecurity or years of practice in digital forensics. A few months of intensive training, in combination with continuous professional education, will largely suffice. Moreover, judges will definitely benefit from cybersecurity education to make better-informed, better-reasoned, and faster decisions in all other cases involving cybercrimes or computed-enabled offenses. For the purpose of judicial training, countries may consider collaboration with international organizations. For example, the World Intellectual Property Organization (WIPO) provides dedicated intellectual property training for judges and magistrates.

Competent courts should leverage the requirement of proportionally, described in the previous section of this framework, and consider several interconnected factors when granting or denying a permission for a cyber operation by police. Firstly, judges shall critically assess whether the operation in question objectively meets the necessity requirements, as well as consider the rationality and practicality of the operation under the circumstances. Secondly,

courts shall state on the permissible technical and operational elements of the investigation including but not limited to the targets, scope, and methods of lawful hacking, which are discussed in a detail in the next section of the framework. Third, the duration of a lawful hacking campaign is pivotal for its eventual success or failure: a deficiently short cyber operation will likely make it unavailing, whilst offering no better privacy protection to the suspect. Similarly, a clearly excessive duration of the operation may later be challenged in court, and also indirectly cause a suboptimal quality of work by relaxed cyber detectives. The court's primary role should be to find the optimum duration of cyber operation to, on the one hand, comprehensively meet the goals of the investigation and, on the other hand, to protect the suspect and any concerned third parties from the unnecessary infringement of privacy and other possible detriments.

As an extra measure of precaution, it may be desirable that, once a cyber operation is completed by police, the public prosecutor in charge should provide a brief summary and the outcomes of the operation to the judges who delivered the authorization to proceed. This will enhance accountability and bolster diligence and care by law enforcement officers in charge of cyber operations, knowing that their actions will be promptly scrutinized by court for adherence to the initially authorized scope and hacking methods. Moreover, by analyzing the reports and eventual success rate of cyber operations, judges may better calibrate their future decisions by allowing more leeway or, contrariwise, by turning the regulatory screw when approving or denying motions to authorize cyber operations.

To avoid bureaucracy and its counterproductive derivatives—such as delays, substandard quality of execution, increased costs of investigation, and missed opportunities to solve serious crimes—judicial approval of cyber operations may provide some reasonable exceptions for urgent investigations. For instance, a public prosecutor may authorize a cyber operation without

first going to court, however, if within a few days the operation is not retroactively approved by the competent court, it must be terminated without delay, and the integrity of digital evidence collected so far must be securely destroyed. Prosecutors may also be subjected to an annual limit for the self-approved investigations they command in cyberspace to avoid conversion of this exceptional route into a default mode of operations in apparent independence from the judicial branch.

§ 4.2.5 Targets, Scope, and Duration

For the purpose of this framework, a "target" shall mean an individual or legal entity whose electronic equipment may be targeted by lawful hacking within criminal investigations by police. Practically, the target selection process forms the very foundation of a cyber operation's legality: a shaky foundation may spoil the entire investigation and cause irreparable damage to innocent third parties. An excessive, as well as incomplete, list of targets may undermine the ultimate success of a cyber operation. For instance, the more suspects are targeted, the greater are chances that one of them will spot the unusual network activity, attribute the intrusion to a possible investigation by a law enforcement agency, and then rapidly notify accomplices to disconnect all their electronic devices from the Internet and wipe out any incriminating evidence. Whilst an exposed cyber operation can temporarily disrupt ongoing criminal activities, but very soon it will rather increase and enhance the anti-forensics tactics deployed by the alerted offenders, ballooning the complexity and costs of further investigations.

Contrastingly, inflexible or overly formalistic restrictions on legally permitted targets (e.g., a flat exclusion of third parties) may also be detrimental for cyber investigation and the interests of justice. For example, key suspects or culprits may have no incriminating records whatsoever on their digital devices, but their suppliers of illicit goods may possess an immense

volume of inculpatory electronic evidence sought by the prosecution. Therefore, setting formal caps on, or narrowing down, the list of lawfully permitted targets may eventually nullify the overall utility of cyber operations.

Of course, targeting innocent third parties should be permitted only under extremely urgent and absolutely exigent circumstances, accompanied by an obligatory notification upon completion of the operation and monetary compensation for all damage caused, if any. Likewise, a prohibition to target CNI, the infrastructure of foreign governments or humanitarian organizations, or devices operated by young kids shall be implemented into the legislation in a piercingly clear manner. Notifications to the affected parties are discussed in the next sections of this framework. To find the right balance when defining the scope of cyber investigations, national legislation on lawful hacking may consider the remoteness of a target to the investigated crime, as well as the target's overall good faith. For example, much stronger protection should probably be given to a legitimate hosting provider that is occasionally used to store illicit materials than to a clandestine hosting company, which has expressly advertised itself as a perfect place to anonymously store outlawed materials and promised to ignore all requests coming from any authorities.

Another factor to consider is the legitimate interest of the targeted third party in preventing the penetration of cyber detectives into its systems. As an example, a suspect's employer may have from little to no interest in preventing or refusing a remote search of a corporate laptop exclusively utilized by the suspect. However, in the very same case, the employer's legitimate interest in the inviolability of its central backup system—storing, among other things, the same evidence as available on the suspect's laptop—should be respected to the utmost extent. Therefore, the legislation and concomitant judicial oversight should allow a

reasonably flexible selection targets within cyber investigations, probably without setting any absolute limits, whilst invariably and meticulously following the proportionality requirement elaborated above.

For the purpose of this framework, "scope" shall be understood as a combination of digital devices and all other electronic equipment owned or operated by targets of lawful hacking. In addition to the hardware scope—represented by specific electronic devices or physical IT infrastructure—legislation should also address a permissible data scope, which would define the "soft" perimeter of remote search, such as stored data or live communications that may be searched and intercepted. The legally permitted scope should be saturated with the notion of proportionality to the fullest extent possible, for instance, fishing expeditions by police shall be expressly outlawed. To further illustrate the point, if electronic evidence is available on a suspect's laptop sufficient to clear the investigated crime, then hacking into the suspect's smartphone—in attempt to discover unknown or additional offenses—must be prohibited. Analogously, if police investigate a proliferation of child pornography or drug trafficking, they may search the suspect's inbox for certain keywords, images, or email addresses, but shall refrain from seeking emails containing tax declarations or privileged communications with the suspect's lawyer for the purpose of uncovering a hypothetical tax evasion. Notably, the foregoing shall not automatically preclude usage of accidentally, albeit lawfully, extracted digital evidence of other crimes committed by the suspect or third parties—if the evidence was found within the permitted search perimeter. Finally, national legislation on lawful hacking shall incorporate special protection for regulated professions including but not limited to lawyers and medical doctors, as well as for any digital communications of the suspect with those professionals when such communications are legally protected by a privilege. Special protection should likewise be

contemplated for journalists and their sources, politicians, lawmakers, and other individuals who enjoy additional protection in their home jurisdiction as a matter of public policy or law.

For the purpose of this framework, "duration" simply refers to the timeframe during which a lawful hacking operation may be executed. Its apparent simplicity may be deceptive, but its incorrect calculation can be fatal for an entire investigation. Consistent with the above-mentioned requirements to properly define the target and scope of a cyber operation, its duration shall be defined through the prism of the proportionality requirement. Based on the researcher's professional experience, determining the proper duration may necessitate a considerable experience and skill. For instance, a court may authorize a two-week remote penetration into a suspect's computer for search and seizure of electronic evidence stored on, or accessible from, the device. If at the very end of the authorized search period, law enforcement agents finally manage to access the suspect's iCloud backup and start downloading it—but eventually restarting the download and finishing it in a couple of days—the admissibility of files and artifacts extracted from the backup may be challenged in court as products of excessive and unwarranted search. Opposingly, a disproportionally long duration of remote search is equally hazardous, not only because of the foreseeable infringement of the suspect's privacy and other rights, but also because the longer the law enforcement officers stay in the system, the more irrelevant data they will likely collect, eventually wasting their time on superfluous data triage and redundant analysis. To address these challenges, national legislation on lawful hacking may impose a fixed cap on the duration of cyber operations, which can be subsequently prolonged on the same conditions as during the initial application required to commence the cyber operation.

In sum, all investigations by lawful hacking are technically and operationally unique. They require a context-aware approach from the supervising judge, whose authority shall

originate from sufficiently precise, but reasonably flexible, legislation in relation to the target, duration, and the scope of permissible lawful hacking. Some *marge de maneuver* therein is critically important for successful cyber investigation. The legislation may, likewise, include some narrow exceptions allowing cyber detectives to temporarily transcend the court-authorized borders of a cyber investigation case of emergency or unforeseeable circumstances justifying a pivot. Such exceptions should, of course, be subsequently ratified by the court as soon as practical, as well as be sanctioned in case of abuse by law enforcement officers.

§ 4.2.6 Hacking Methods and Software

National legislation on lawful hacking should thoughtfully address, among other things, the permitted hacking techniques and tools that can be operationalized by cyber detectives without endangering the security of their own agency, of the suspect, and, of course, of any third parties. In light of the rapid technical progress and ongoing evolution of hacking techniques, the legislation on lawful hacking shall refrain from using a strict language to describe hacking methods or incorporating a list of authorized software tools or frameworks. Instead, it shall focus on their innate properties, characteristics, and capabilities to cause certain effects on digital equipment or electronically stored data. Similarly, overbroad or ambiguous definitions will give too much leeway and probably cause excessive or collateral damage when running investigations in cyberspace. Consistent with the previous sections of this framework, the hacking techniques and tools used by law enforcement agencies within criminal investigations shall be subject to strict proportionality requirements. In the paragraphs below, the main considerations in relation to hacking methods and software tools, ranging from exploits to spyware, are discussed.

First, usage of any malware, having contagious self-propagation capabilities, shall be prohibited by national legislation on lawful hacking. As otherwise, sooner or later, police will

inevitably become accountable for a global epidemic of malware, causing multi-billion damages, and likely entailing severe consequences under international law. Technically, in a properly orchestrated hacking operation by law enforcement, the chances that cyber detectives may need a spyware with self-propagation capabilities border on zero. Importantly, the pejorative notions of self-propagation and contagiousness should not be confused with the necessary persistence capabilities of investigatory spyware. Most cyber operations that target suspect's computers, smartphones, wearable gadgets, or servers primarily aim to exploit a known software vulnerability and then secretly install persistent spyware to remotely control and monitor the device, unbeknownst to the suspect. Almost without exception, persistence is required by default and by design to achieve the legitimate goals of the cyber operation. Otherwise, after every reboot of the surveilled device, a new hacking attempt would be required, recklessly wasting police resources and gradually increasing the chances of raising the notice of the suspect.

Second, national legislation should prescribe a general requirement to minimize the usage of any hacking software, spanning from trivial exploits to advanced spyware, that has not been properly tested for reliability or is known for occasionally causing some random damage to the targeted system. For instance, certain untested exploits may crash the system, causing possible loss or corruption of data, being particularly problematic when the attacked IT infrastructure is shared by several tenants unrelated to the investigated crime. The notion of harmlessness, however, shall not be conceived in the absolute sense. For example, during a de-installation, some spyware may wipe out temporary or log files generated by unrelated third-party software, aiming to hide its own activities after leaving the surveilled system. Even if such actions are theoretically destructive, in practice, the material damage will unlikely ever be noticeable. Moreover, some advanced variations of spyware may even purposely leave well-known artifacts

belonging to other malware, with the underlying purpose of hindering attack attribution in the case of subsequent detection. Although commonly leveraged by cybercriminals, the deliberate misattribution tactic—aimed to usurp the identity and frame up an identifiable and well-known cyber threat actor—shall, obviously, not be utilized within lawful hacking operations as a matter of ethics and professional integrity of law enforcement troops. However, some changes to suspect's devices, which are reasonably required to successfully complete a cyber operation, should be explicitly permitted when the proportionality requirement is duly respected. Furthermore, some cyber campaigns may even necessitate a temporary takedown of a suspect-operated wireless router or Domain Name System (DNS) server to successfully compromise another device of the suspect. Conditional to the harmlessness of the attack for any third parties and the reliability of the means to continually control the attack's scope and perimeter, such intrinsically harmful attacks should not be banned by lawful hacking legislation. Nonetheless, the legislation should impose comprehensive reliability requirements for hacking software, in parallel, leaving some reasonable *marge de maneuver* for cyber detectives. Illustratively, a new major version of an operating system will probably require a broad spectrum of modifications to most of the existing spyware, even if it has been working impeccably on previous releases of the same operating system. Trying to backdoor a new system with an old or untested version of spyware may, in the best-case scenario, be futile or, in the worst-case scenario, crash the remote system, expose the attack, and ruin the entire operation.

Third, a mandatory certification or an in-house-only development of hacking tools, exploits, or spyware will likely be counterproductive and may bring more harm than good. For instance, some cyber operations may urgently require written-from-scratch software capable of remotely compromising and then maintaining control over an atypical IoT device or a brand-new

wearable gadget. In other cases, a modified version of spyware designed to stay invisible within a dynamically changing multicloud environment, to use a custom-made obfuscation technique, and to evade detection with an unusual covert channel to exfiltrate the data may also be rapidly needed within an investigation. In both hypotheticals, a formal certification of the hacking software will likely be disproportionally expensive, lingering, and impractical. Likewise, in such cases, acquisition of the requisite cyber instruments from trusted third parties may be the fastest and most cost-efficient option. Notably, the wide range of third-party risks is discussed in the next sections of this framework, but here it is pertinent to mention that national legislation should contemplate getting access to the source code of external tools and software used in lawful hacking operations. The operationalization of proprietary black-box hacking tools and especially persistent spyware that cannot be inspected by law enforcement experts when needed represents a slippery slope that should be avoided whenever possible. For obvious reasons, cyberwarfare vendors may be reluctant to disclose their trade secrets without a tenfold price increase, however, a middle-ground solution can possibly be found with a source code escrow. Law enforcement will have no access to the source code by default, but in case of a reasonable doubt that the software in question has violated its terms of service (e.g., being equipped with undocumented features or grabbing more data from suspect's devices than initially declared), the source code will be disclosed by a mutually trusted third-party for the eventual investigation and calculation of monetary damages if the product's terms of service were knowingly violated by the vendor. This will likely bolster accountability and deter carelessness among software suppliers. Further details and precautions are discussed in the dedicated section of this framework below.

Fourth, the hacking methodologies and specific features of spyware shall simply be wrapped into the proportionality requirements, without compiling protracted and subjective lists

of "good" or "bad" technical features. Some laser-focused exceptions may, however, be implemented by legislators, for instance, by setting a ban on attacks that may disrupt devices implanted into a human body and cause serious risk to a person's health or even provoke a fatal outcome. For other cases, respect of the proportionality requirement shall normally suffice. For instance, interceptions of data from a microphone and web camera on a suspect's device, where some financial documents on the laptop's hard drive are the sole evidence sought by prosecution, will certainly be disproportional. By contrast, when the suspect's laptop is merely used to monitor and record the suspect's secret phone conversations on planning dangerous crimes, taking place in the same room from unknown or unidentifiable cellphones, usage of a microphone will certainly be adequate and proportional, but probably not of the camera. Therefore, national legislation on lawful hacking should provide clearly discernible borders of conceptually allowed hacking methodologies and characteristics of spyware but, at the same time, leave a sufficiently broad space for creative exploitation and backdooring techniques when the proportionality requirement is duly preserved by cyber detectives.

Fifth, a legal prohibition on the exploitation of zero-day vulnerabilities may rather support goals opposite to the safeguarding of digital society, especially when dealing with small vendors or unpopular software products. As a zero-day vulnerability for such product may cost less than a thousand dollars, law enforcement agents may simply buy and then disclose the vulnerability, and once the flaw is acknowledged by the vendor and cybersecurity community, rapidly exploit the unpatched suspect's system before the official patch is released and installed by the suspect. Regrettably, in most cases, small vendors will either spend many weeks to release a patch or even release no patch at all, leaving many Internet-facing systems vulnerable and thereby provoking a wave of successful intrusions by nimble cybercriminals. The preceding,

however, does not mean that the nature of exploited vulnerabilities should be exempt from the proportionality requirement. For instance, exploitation of a remote zero-day vulnerability in a mega-popular software product shall be avoided whenever possible, as chances that the attack will unintentionally expose the vulnerability to third parties are usually pretty high, causing a domino effect of disastrous data breaches by cybercriminals once the vulnerability leaks into public domain. In some cases, exploitation of such zero-day vulnerability may safely take place after notifying the vendor, just after a security patch is released and globally promulgated. The suspect will highly unlikely update its system within minutes of a new security alert, whilst millions of innocent users will probably install the patch before cybercriminals commence exploitation in the wild. In continuation, under a specific set of circumstances, when the risks of a zero-day flaw disclosure are minimal and can be controlled with reasonable certainty (e.g., by a rapid wipe of all exploitation traces including network logs if accessible), a zero-day vulnerability may, arguably, be legitimately and safely reused in future operations without notifying the vendor. However, once again, when regarded through the lens of proportionality, the foregoing can hardly be applicable for a critical vulnerability that can exploited remotely in a default configuration and without authentication, affecting, for example, billions of iPhone or WordPress websites. Precautions related to the storage and acquisition of zero-day vulnerabilities are discussed in the next sections of this framework.

Finally, post-operation activities shall equally be imposed by national legislation on lawful hacking. Perhaps the most important aspect to consider by legislators herein is the safe and complete removal of spyware or other software from the impacted systems, which has been deployed by police investigators during a cyber operation. The impacted systems are to be restored to their original state whenever technically possible and not excessively burdensome.

The system cleanup and restoration will, self-evidently, be favorable for the suspect and any concerned third party, as well as for law enforcement agencies: any remaining traces of intrusion may allow a reverse engineering of police spyware or hacking methodologies, potentially disclosing valuable knowledge or technical insights to organized crime for subsequent misuse, reselling, or active defense from similar investigations by police. In sum, all possible modifications made to the suspect's or a third-party's system during a cyber operation shall be reverted to the maximum possible extent, but without overly strict formalities.

§ 4.2.7 Digital Evidence Preservation

The irreproachable collection, preservation, and authentication of electronic evidence should cement the pillars of national legislation on lawful hacking. The underlying forensic processes and technical procedures, however, do not necessarily need to be created from scratch. First, lawmakers should assess the compatibility of lawful hacking legislation with existing domestic laws or rules administering the admissibility of evidence in courts, namely digital evidence within criminal proceedings. Second, to preclude foreseeable challenges to the admissibility of adduced electronic evidence, lawmakers may consider incorporating a set of time-proven and science-backed digital forensics and electronic evidence management frameworks into lawful hacking legislation, for example, by picking some of the forensic standards and guidelines discussed in Chapter 2 of this dissertation. Being already tried within a domestic judicial practice and forming an integral part of national jurisprudence, the frameworks can elegantly yield and incorporate the existing wisdom, science, and jurisprudential considerations into the nascent body of lawful hacking legislation, without reinventing the wheel.

To ensure the technical appropriateness of evidence management, the legislators should, before prescribing a specific framework, nominate an interdisciplinary expert commission to

conduct an in-depth review of the existing jurisprudence on the admissibility of digital evidence in domestic courts and to suggest the most appropriate framework, or a set of frameworks, tailored for their home jurisdiction. The expert commission should bear in mind both the particularities of their national judicial practice and the technical fitness of the suggested frameworks when regarded through the scientific prism of the collection, preservation, and authentication of digital evidence gathered by the means of lawful hacking, which may considerably deviate from a traditional digital forensic environment (as explained in Chapter 2). Upon completion of the research by the expert committee, the lawmakers may simply incorporate the handpicked framework into their domestic legislation on lawful hacking by reference. Importantly, the legislation shall instruct cyber detectives to coherently follow the most recent versions of the framework—unless the newer version is found incompatible with the established practice or law—to ensure that law enforcement keeps pace with the evolution of forensic science.

In relation to digital evidence preservation, this research also suggests an extra layer of special precautions when conducting cyber operations designed to investigate particularly serious crimes or offenses implicating arrests of kingpins and leaders of criminal cartels. Law enforcement agencies should be prepared in advance to face skilled and savvy opponents in court, ranging from legendary criminal defense attorneys to venerated digital forensics experts and legal scholars, hired and generously paid by the influential defendants. Thus, a mere compliance with one or several digital forensics frameworks may likely fall short of overcoming a stonewall defense's arguments and avalanche of thought-provoking objections. Therefore, in addition to the rigorous adherence to existing forensic frameworks, lawful hacking operations should contemplate supplementary controls to back the legality of the entire lawful hacking

process and to dispel any reasonable doubts concerning integrity or authenticity of the collected evidence. Those controls are briefly discussed below. Firstly, the researcher suggests deploying one of the widely available computer activity tracking software to comprehensively record all actions performed by cyber detectives. The recording shall, among other things, log every keystroke, each non-system file modification, and all user-generated network packets sent or received, as well as recording the detective's computer screen in real time. Each cyber operation shall start with a video recording of a brief introduction made by the detective in charge, concisely explaining the context, the process, and the next steps (without over-disclosing technical or other sensitive details). Then, the cyber detective may review the configuration of its computer and any virtual machines running thereon, namely demonstrating their network configuration, date and time, and DNS servers to preclude possible accusations of setting up the scene in an artificial environment or tampering with digital records. To protect the detective's privacy and safety, its voice shall be altered and face hidden, alongside any other details that may serve to uncover the detective's identity. In particularly serious or contentious cases, the installation of a clean system from an authenticatable, trusted, and verified source may be required and duly recorded at the very beginning of operation to negate all imaginable accusations of using an altered operating system with hidden functionalities.

Secondly, the cyber detective, without exposing its identity, may be filmed from behind or from the top while executing the cyber operation, so that the external video recording of the detective's computer screen and keyboard can later be synchronized with the recorded digital snapshot of the operation to cross validate its integrity and authenticity. Thirdly, to avoid excessive costs of storage and unnecessary triage, only the essential parts of a cyber operation shall be preserved for court proceedings, for instance, several failed attacks, exploit payload

customization, or the entire reconnaissance stage may be omitted. Likewise, any parts of the recording that may, inter alia, disclose zero-day vulnerabilities or lead to another undesirable outcome, shall be either removed completely—if not crucial for the essence of operation—or marked as ultrasensitive, thereby obtaining a special protection in court if demanded to be disclosed by the defense. Eventually, the defense council and any third-party experts will have an extra duty to never disclosure or reuse the ultrasensitive evidence, or any parts thereof, under the penalty of losing their license to practice and facing a hefty monetary fine. Additionally, any vexatious demands of superfluous technical examinations made by defense—merely designed to slowdown the judicial proceedings—may be severely sanctioned if compatible with the national criminal procedure law. For example, if no violation of law by cyber detectives is eventually found, the defendant may be required to pay a treble compensation of the costs incurred by the prosecution to disincentivize deliberate abuse of law aimed to sabotage the trial process. On the other side, if a violation of the law is found and proven, the defense shall be eligible for the full compensation of all reasonable costs and expenses, serving as a deterrent against police abuse and prosecutorial misconduct.

Upon the successful completion of a cyber operation, the recordings and the seized digital evidence shall be reliably authenticated and placed into a sealed and secure vault for the upcoming trial. Copies of the recordings, which do not contain sensitive personal data or other information that may deserve protection as a matter of law or ethics, may also be used for internal training within the law enforcement agency in charge of lawful hacking to brainstorm, improve, or develop novel techniques of offensive operations in cyberspace. The secure disposal of the recordings is discussed in the upcoming sections of this framework.

In sum, when swimming in the shark-infested waters of organized crime prosecution, the foregoing setup of a forensically sound lawful hacking environment will likely be resilient even to the sharpest bites and most inventive or perfidious arguments of defense made in court. The process of digital evidence collection, preservation, and authentication shall, of course, be continually improved and updated whenever necessary. Procedurally, the foregoing suggestions may either be incorporated into the main body of lawful hacking legislation or, depending on the jurisdiction and its particularities, added to the criminal procedure law or other relevant pieces of national legislation.

§ 4.2.8 Notification of Affected Parties and Compensation

National legislation on lawful hacking should aim for a seamless and simple implementation of notification requirements to all parties materially affected by law enforcement investigations in cyberspace. In many jurisdictions, such provisions already exist in a general form, for instance, as part of the enacted criminal procedure law or other statutory acts, to address situations when similarly intrusive but less technically sophisticated methods are deployed by police detectives. Lawful hacking, however, is more nuanced compared to the conventional investigatory instruments that traditionally require notifications, such as GPS tracking, interception of postal correspondence or phone calls. Commonly, notifications to suspects are mandatory and must be performed as soon as practical, however, they can be postponed or even selectively waived—subject to a court approval—if the notification may jeopardize the interests of justice, endanger witnesses or law enforcement officers, hinder further investigations, or simply bring no value whatsoever to the suspect whose privacy and other rights were not materially infringed.

In view of the considerable heterogeneity of national legislation and peculiar procedures in relation to the notification requirements within criminal investigations, it would be an arduous task to draft a universal recommendation on the process in this framework. Nonetheless, several general aspects and essential considerations, as applicable in most jurisdictions, should be considered by legislators when enacting or amending their national legislation on lawful hacking. The principal considerations are briefly discussed below.

First, a competent court shall assess and consider whether a notification may expose valuable investigatory techniques or methods, for example, when cyber detectives could not clean up their digital traces or when other reasons exist to believe that logs of the cyber operation may be recovered from the suspect's device or a third party, for instance, from a cloud service provider. Of course, the requirement of proportionality elaborated above shall be used as a compass to impartially balance the legitimate interests of the suspect and prosecution. Courts should, however, foresee that dealing with organized crime and transnational criminal cartels, which require and justify the deployment of lawful hacking operations, implies that any notification will likely entail a vigorous reverse investigation by the culprits and their acolytes, who can afford to hire cybersecurity and digital forensics experts of the same or even better qualifications than those of law enforcement agencies. Eventually, external experts hired by organized crime may reverse engineer the investigatory techniques used by police and, among other things, set traps and honeypots to detect or obstruct upcoming cyber operations. Additionally, villains may simply sponsor an alarmistic campaign in the local media to overexaggerate, dramatize, and catastrophize police hacking, with the insidious goal of repealing lawful hacking legislation under the mounting pressure of simmering public outrage. Those

particularities should be mindfully contemplated by the court before ruling on the dispense of a notification.

Second, in the labyrinthine realm of lawful hacking, third parties may be inadvertently and often unpreventably impacted by the legitimate cyber operations conducted by cyber detectives against serious or organized crime. Theoretically, even using or passing through a third-party IT infrastructure, even for activities that are harmless per se, may speed the depreciation of the electronic equipment and increase billing for electricity or pay-as-you-go cloud services. Unquestionably, any significant and material damage—even if invisible and undetectable by the affected third party—must be compensated in full to avoid creation of a World Wild West of frivolous police raids on the Internet in conscious disregard of third-party property rights.

Third, the compensation rule, however, shall not be categorical, mechanical, or absolute. For instance, several thousands of dollars in damages inflicted upon a small family business are to be compensated in one way or another, whilst the same damage suffered by a multibillion corporation may be exempt from compensation when such exemption is indispensable to protect the vital interests of justice or innocent third parties. That is, of course, not to suggest that wealthier entities deserve less protection: alternative and investigation-friendly ways of adequate and fair compensation may be contemplated. For example, major service providers, which are likely to be impacted by hundreds of cyber operations per annum due to their inadvertent popularity among criminals, may receive a consolidated annual compensation for relying on their computational or network resources without prior authorization and without disclosing sensitive technical details or the scope of the cyber operations. The provision of monetary compensation should be conditioned on a duty of strict confidentiality ensuing from a contract: before entering

into the contractual agreement to keep the very fact of compensation confidential, providers will not know even the proposed amount. The proposal to enter into a confidentiality agreement can be made by informal channels, also providing a mutually beneficial opportunity to negotiate and amend the agreement, for example, by requiring the police to give notice to the provider if their cyber detectives accidentally spot or become aware of a critical security flaw or misconfiguration in one of the provider's products used by millions of subscribers. The underlying purpose of alternative methods of compensation should be to foster public–private collaboration, whilst duly preserving property and other essential rights, as well as complying with the existing statutory and case law in relation to expropriation by the government. Once again, the entire process shall rely on, and be inspired by, the requirement of proportionality, as well as be consonant with the jurisdiction-specific legal doctrines and practice.

§ 4.2.9 Internal Security Controls

A data breach of the national law enforcement agency in charge of lawful hacking may entail a cyber havoc on an international scale: not only will governmental cyberwarfare be stolen and potentially resold to nefarious cybercriminals, but numerous confidential dossiers of complex or transborder investigations of serious crime will be misappropriated. In the best-case scenario, the stolen data will be exploited to blackmail the government, extorting a ransom that will, however, provide no guarantee whatsoever that in the future the data will not be resold or even publicly exposed. In the worst-case scenario, organized crime and criminal cartels would be among the wealthy buyers of the stolen data, exploiting its invaluable intelligence to exterminate undercover law enforcement agents or police informants, as well as to fortify their anti-investigatory tactics and possibly render future cyber investigations fruitless or make their costs exorbitant. Therefore, national legislation on lawful hacking should not simply rely on any

existing laws that regulate data protection in governmental agencies, but mandate a special data protection and information security regime to be established within the governmental units in charge of lawful hacking and any other state bodies with a privileged access to the operational, technical, or otherwise sensitive data of cyber operations. Depending on the jurisdiction and particularities of the domestic legal system, the special data protection regime can, of course, be elegantly incorporated into a separate data protection law if such legal construction is more practical or manageable.

Obviously, the special data protection regime, while necessitating an express incorporation into national legislation on lawful hacking in one way or another, does not require to be invented from scratch by lawmakers. Instead, it may be based on well-known and thoroughly validated by practice cybersecurity frameworks or guidelines published by competent governmental bodies, such as the Cybersecurity and Infrastructure Security Agency (CISA) in the United States or by the National Cyber Security Centre (NCSC) in the United Kingdom. The legislation shall, however, unambiguously emphasize that the data protection regime must continually follow the evolution of technical progress and comply with the most recent version of the selected frameworks unless there is a compelling reason to deviate. Likewise, the framework, or a collection of interconnected frameworks, should comprehensively address the following non-exhaustive list of interconnected areas: risk management and threat modeling, data classification and IT asset inventory, physical security, strong authentication and access management, protection of stored data and data in transit, human security and internal employee vetting, third-party risk management, Secure Software Development Lifecycle (S-SDLC), software acquisition and license management, incident forensics and response, cyber threat intelligence, continuous security monitoring and auditing of the implemented controls, privacy

and personal data management, and employee security training and awareness. Certain of these areas deserve a dedicated exploration and will be discussed in the following sections. To add an extra layer of protection and oversight, bi-annual audits by an impartial governmental body should probably be directed by lawful hacking legislation, enhancing the accountability and auditability of the data protection regime at the national law enforcement agency entrusted to lead lawful hacking operations within criminal investigations.

§ 4.2.10 Data Retention and Deletion

The duration and secure disposal of electronic evidence collected within lawful hacking operations by law enforcement is crucial to the entire process. Although being an integral part of the data protection regime elaborated in the previous section, data retention and deletion procedures deserve a dedicated mention due to their critical importance and high sensitivity. Procedurally, to avoid incompatibility or overlaps with the long-established provisions of the national criminal law, all electronic evidence shall be securely stored and preserved for as long as provided by the enacted criminal procedure law in relation to evidence preservation within criminal proceedings. In cases when a court orders a termination of cyber operation for lack of a legal basis to deploy or pursue the intrusive cyber surveillance, the information already harvested during the non-approved timeframe of the operation must be undelayedly deleted in an unrecoverable manner, including subsequent removal of the data from backups within feasible.

The foregoing issues are fairly straightforward and uncomplicated compared to the intricate question of how long the ancillary collected metadata or artifacts gathered during lawful hacking operations should be kept if they are not designed to, and probably will not, be produced in court. To escape the slippery slope of two paralleled data retention regimes with a blurred separating line in between, police cyber investigators should be simply required to preserve all

electronic evidence and any auxiliary information related thereto if its disclosure may be reasonably expected to be needed or lawfully requested in court for cross examination by independent experts mandated by defense. Everything else—with some narrow exceptions for purely technical materials that do not contain personal information or other sensitive data and being designed, for example, for internal training or supervising cyber operations—must be securely deleted as soon as the operation is over.

To alleviate the burden of lawmakers, the legislation may simply require the nomination of an internal Data Protection Officer (DPO). The DPO will administer the technicalities of drafting and continuous improvement of the agency's data retention and privacy protection policies, defining the requisite scope, nature, and format of the retained data, whilst acting strictly within the permitted borders and in compliance with the existing law in relation to data protection applicable to the agency. Of note, the data protection policies must expressly and unconditionally prohibit all access and any use of the stored data unless directly required for the performance of direct professional duties by law enforcement officers. All access attempts, including failed ones, should be logged and painstakingly audited on a regular basis to prevent frivolous or unauthorized access to confidential and sensitive data of investigations by overly curious agency employees. The policy must be holistically enforced with appropriate security controls, regular audits for violations, and contractually imposed fines or more severe penalties for unwarranted or excessive access. Finally, a special legislative protection for the DPO role may be inspired, for instance, by the GDPR protections for corporate DPOs, who are shielded from arbitrary discharge and other repercussions whilst duly performing their professional duties.

§ 4.2.11 Subcontracting to Third Parties

In the era of spiraling shortage of cybersecurity talent, an in-house development of advanced spyware, exploit kits, or hacking tools may be cost-prohibitive for law enforcement agencies in most countries, let alone research for zero-day vulnerabilities in popular software, firmware, or hardware. Furthermore, some cyber operations may occasionally require a unique set of tools or custom-made exploits, which are otherwise never needed for the daily lawful hacking activities, and thus may be missing in the cyber arsenals of law enforcement agencies. Reflecting the contemporary needs of investigatory operations in cyberspace, there is a growing trend on grey and black markets to lease spyware and exploit kits, instead of selling them at much higher prices. Therefore, certain laser-focused investigatory cyber operations, for example, involving a remote takeover of previously unseen electronic devices, requiring a rare skillset or customized exploits aimed to pierce a multilayered cyber-defense, may be partially or entirely outsourced to trusted private companies to save time and budget, preserving taxpayers' money for a better use.

In sharp contrast to the obvious economic, technical, and operational benefits of subtracting, it may also be an abundant source of impermissible violations of human rights and freedoms, may lead to leaks of highly confidential data, misappropriation of hacking tools, or intelligence by organized crime, well as may cause countless other undesirable outcomes usually associated with the risks of an inadequately managed supply chain. Hence, the entire process of dealing with any third parties, from the initial request of information to the eventual secure disposal of collected data, must be thoroughly regulated by national legislation in congruence with the proportionality requirement, as discussed below.

First, ownership and employee due diligence is to be imposed in a holistic but calibratable manner. For instance, some states, including Hong Kong and South Korea, do not provide conventional checks of individual's criminal records, but offer some alternative ways to assess possible risks associated with an individual's background. Therefore, hardcoding into the text of legislation any inflexible requirements may rather hinder the due diligence or simply provoke the acquisition of less efficient tools from less competent vendors that are, however, capable of meeting procurement formalities. Furthermore, the due diligence of vendors' individual employees is unlikely to bring any value in isolation from other checks. The chances that key developers of powerful hacking software will turn out to be malicious insiders, recruited by foreign intelligence or organized crime, are relatively insignificant. Conversely, a plethora of risks of considerably higher impact and frequency may originate from company-wide information security deficiencies, overall carelessness, or internal mismanagement. Among the foreseeable examples are poorly or incompletely implemented internal security controls, an absent or unenforced Supply Chain Risk Management (SCRM) program when dealing with subcontractors, flawed segregation of duties, or overbroad internal access permissions that allow even interns, accountants, or sales executives to access corporate crown jewels—just to name a few malpractices that may open a Pandora's box of disasters.

Therefore, in addition to individual risk scoring, the enterprise-wide due diligence of suppliers should figure among the foundational precautions when dealing with third parties. The due diligence shall likewise include a multistage inspection of, among other things, all relevant data protection and privacy policies; most recent internal and external audit reports pertinent to the analyzed security controls; the internal procedures governing employee hiring, vetting, and dismissal; and copies of internal records of the most recent incidents involving major violations

of the existing policies or procedures. Additionally, the due diligence exercise should shed light on the vendor's financial solvency, examining not just its annual financial reports but the current cash flow, liquidity, and any upcoming financial obligations: for example, repayment of loans that may increase vendors' financial instability and bolster the risks of misconduct or susceptibility to external blackmailing. For particularly sensitive or otherwise critical missions entrusted to third parties, such parties may be required to maintain a deposit in a bank that will serve to cover contractually agreed damages in case of negligence or misconduct by the supplier or its own subcontractors. Finally, a letter from the vendor's board of directors, structured in a way that would trigger a personal liability of each board member in case of deliberate falsity, is required to unambiguously confirm that the company has not been involved in, and has no reasonably foreseeable future risks of being involved in, any civil litigation or criminal probe that may jeopardize the integrity or undermine the quality of products and services supplied to the agency. Finally, the supplier shall contractually commit to notifying the agency as soon as practical about any already-occurred, impending, or reasonably foreseeable risks and threats under the penalty of a formidable monetary fine in the case of non-compliance. Procedurally, the nuances and operational details may be left to the discretion of the agency, to avoid overregulation and pollution of the national lawful hacking legislation with superfluous technicalities and micromanagement.

Second, the overall legality of dealing with specific countries, individuals, goods, or methods of payments should be prescribed by the legislation in conformity with the national legal system. Coherently with the foregoing provisions, the threshold of legality should be fixed in a sufficiently high but adjustable manner without categorical bans. In some countries, for example, payments in cryptocurrencies may be prohibited or may require a special license from

the local regulator. Illustrating this point in further detail, payment to unknown entities—mostly when dealing with one-time transactions on the Dark Web—implies the unknowingness of the supplier's true identity, creating a risk of payment to sanctioned states or embargoed entities. Therefore, legislators should adjust their national lawful hacking legislation, bearing in mind the particularities of their domestic legal system and considering provisions of both procedural and substantive law. Importantly, occasional purchases of tools or services on the Dark Web, or on other non-regulated underground markets, should not be uniformly outlawed: Sometimes, a test transaction may be an inalienable part of the investigation purpose designed to unmask the wrongdoers. In other scenarios, certain indispensable tools, data sets, or intelligence— whilst not constituting products of crime—are commercialized only on grey markets and can be paid solely in cryptocurrencies. Therefore, the more *marge de maneuver* cyber detectives will be afforded by law, the more efficiently and effectively they will combat serious crime. That being said, the foundational requirement of proportionality shall be unconditionally respected, carefully balancing privacy and other individual rights with the legitimate interests of justice, as well as considering the already-enacted national law.

Third, the supplier due diligence process should be a continuous and continually improved process, adjusted to the nature and risks of the vendor relationship. A one-size-fits-all approach will certainly not fit the governmental need to prevent incidents and violations of law, being either an overkill or a fishing net with holes that are too wide to capture threats. For instance, acquisition of hacking software or spyware will certainly require numerous precautions, including but not limited to on-demand access to the source code and the vendor's contractual warranties of a reasonable quality, reliability, and non-infringement of third-party intellectual property rights. The same transaction may equally include a vetting of the supplier's ownership

and other checks aimed to ascertain that the same spyware has not been sold to the actual targets of lawful hacking or third parties who may, for example, purposefully share it with major antivirus companies. However, blanket background checks on all software engineers may meaninglessly waste time and resources on both sides and, more importantly, provide a false sense of security and cause the eventual ignorance of more relevant risks and threats. By contrast, when hiring an external penetration testing vendor—whose employees will be stealthily penetrating remote systems to seize critical electronic evidence or intercept highly sensitive communications, where the premature disclosure of which to media or third parties may torpedo years of the cross-border investigation and cost the lives of undercover police agents—due diligence must be conducted not only on the penetration testers but also on their close relatives and partners, to the fullest extent permitted by law. Summarizing this section, third-party due diligence shall stand on the inviolable requirement of proportionality, whilst being sufficiently flexible and context-driven. The nature of vendor vetting shall be invariably comprehensive, risk-based, and threat-aware.

§ 4.2.12 Transparency and Statistics

To enhance a sustainable public trust and confidence in lawful hacking conducted by police within criminal investigations, national legislation should elaborate a robust process to transparently and reassuringly disclose police activities in cyberspace. The underlying goal of the process should be to convince common citizens that contemporary cyber operations are aimed solely at protecting society, are thoroughly regulated and administered by law, and are rigorously supervised by the judicial branch of government in an impartial and fair manner to safeguard individual rights or freedoms. To achieve this appealing goal, an annual or bi-annual transparency report on lawful hacking by law enforcement agencies can be published on the

Internet and shared with national media. The report should provide a comprehensive summary of cyber operations conducted by law enforcement agencies to prevent, investigate, and prosecute serious crime, emphasizing its benefits for society and sharing case studies of the successful dismantlement of organized crime groups and solved crimes.

Whilst sensitive operational or technical details shall, of course, not be disclosed in the reports for obvious reasons, it may be a good idea to highlight the gravity of the investigated offenses by providing a table with classifications of the offenses' severity. Additionally, it may be helpful to elaborate the precautions undertaken by law enforcement officers during cyber operations to ensure the non-interference with any third parties to the best possible extent. This can be achieved, for example, through the selective publication of anonymized but detailed case studies designed to guide laypeople through the lawful hacking in a simple and understandable manner. Notably, in jurisdictions where legislation permits citizens to request certain information about governmental activities (e.g., under the U.S. Freedom of Information Act [FOIA] or the Freedom of Information Act [FoIA] in Switzerland), transparency reports shall be prudently designed not to overfeed the reader with hints or creative ideas of what else can be demanded from the government under freedom of information laws.

In continuation, free online trainings, for instance, organized in partnership with a national cybersecurity agency or regulatory bodies, may help to promote information security literacy and empower people to better grasp the essence of lawful hacking through free technical education. Regular nation-wide events for students, who are considering becoming cyber police officers after the college and partaking in the combat against the nefarious hydra of organized crime, may attract additional awareness among their parents and enhance the positive image of cyber police officers and the lawful hacking profession. Better-informed and better-educated

citizens are the most efficient, viable, and sustainable way to transparently inspire trust and confidence in law enforcement activities in cyberspace aimed to protect society.

§ 4.2.13 Independent Oversight

In addition to the judicial oversight described above in this framework, an independent oversight of lawful hacking by police within criminal investigations may also be a valuable mechanism to strengthen the integrity, lawfulness, and efficiency of cyber operations. Such a mechanism may be aptly embodied by a short and flexible provision in national legislation on lawful hacking. For instance, independent surveillance can be performed by an expert committee composed of legal scholars, industry experts and practitioners, lawyers, and human rights advocates, who will be empowered to request supplementary data from the competent authorities upon publication of each periodic report on lawful hacking discussed above. Procedurally, the government should, of course, be empowered to refuse a disclosure of confidential or otherwise sensitive materials at its own discretion, but the legislation should prescribe a duty to act in good faith and duly provide the requested information unless doing so is excessively burdensome or detrimental to the past, ongoing, or future cyber investigations by police. Based on the additional information received, the expert committee shall regularly produce a brief report with its observations, findings, and recommendations for potential improvements, suggesting how to ameliorate the existing technical, operational, or organizational processes of lawful hacking, as well as how to continually provide a better protection for individuals, enterprises, and public entities concerned about lawful hacking activities in cyberspace. The report should have no binding effect, however, after incorporating a preliminary response from the authorities, it shall be distributed to the national media and made public to ensure transparency and awareness.

Depending on the legal and social traditions of a country, members of the expert committee may be discreetly selected by the government from an open list of candidates who can apply themselves or be nominated by anyone online via a dedicated website. Alternatively, each political party may nominate its candidates, for example, in pro rata of their parliamentary seats. The maintenance of equality between the number opponents and proponents of lawful hacking is crucial to ensure an equilibrated and fair process of police investigations in cyberspace that strike the right balance between inviolable civil rights and effective cyber investigations of serious and organized crime. Committee members may be eligible for reelection and subject to the reasonable requirements of academic qualifications or relevant professional experience, good character, and the absence of conflicts of interest. Summarizing this section of the framework, national legislation on lawful hacking should make the independent oversight process simple, transparent, and easily manageable to meet its underlying objectives.

§ 4.2.14 Safe Harbor

Another element of national legislation on lawful hacking that should be expressly addressed therein is a "safe harbor" provision that would protect police officers—who perform cyber operations in compliance with the law and in good faith—from the prosecution for possible violations of antihacking laws, such as the Computer Fraud and Abuse Act (CFAA) in the United States. Most countries, being obliged or inspired by the Budapest Convention, have enacted comprehensive and comparatively strict anti-hacking laws that, among other things, criminalize unauthorized or excessive access to information systems, deletion or corruption of electronic data, and unlawful interference with computerized systems. In some instances, a cyber operation, like any other intrusive investigatory operation in the physical world, may unpredictably lose control and unintentionally cause damage to innocent third parties.

In the future, organized crime will likely amalgamate with cybercrime, creating a powerful criminal synergy that will be able to deploy traps and honeypots to detect and possibly frame police officers. For instance, cyber detectives may gain access to a honeypot, believing that it is the targeted suspect's system and lawfully start searching for suspect's data. They will then stumble upon specially implanted credentials from a cloud storage or third-party service—apparently belonging to the suspect—whilst in reality being stolen from a third party and perfidiously placed on the fake investigated system to frame police officers as the authors of illicit intrusion. Eventually, after accessing those systems and extracting the data, the officers may be charged with violation of anti-hacking laws, depending on the context, jurisdiction, and public policy. Therefore, in light of the mounting sophistication of cyber operations and the growth of concomitant risks, lawmakers should explicitly exempt police officers from any criminal charges for the good faith performance of their professional duties within cyber investigations. Obviously, the foregoing should not be extrapolated to exonerate a deliberate and illicit breach of third-party systems or any other activities that clearly transcend the powers vested upon the officers by the national legislation on lawful hacking.

§ 4.2.15 Insurance

Despite the long list of technical, operational, and legal precautions described in this framework above, a lawful hacking operation may unanticipatedly go wrong, as any other complex process or mechanism in society, spanning from transatlantic cargo transportation to nuclear plant management. To shield the government, and thus the taxpayers, from losing money in case of an unforeseeable and unpreventable incident, the entire process of lawful hacking, or at least some parts of it, should be insured. Due to the novelty of the lawful hacking concept, negotiating a mutually acceptable contract with an insurance company will likely consume much

time; however, this duty may be flexibly prescribed by national law on lawful hacking, leaving space for creative negotiations with the insurance.

Eventually, even if due to some circumstances beyond the reasonable control of cyber detectives, a suspect or any third-party suffers a material or other compensable form of damage, they can be compensated by insurance in an expediated manner. Likewise, if the damage is suffered by the law enforcement agency, it will be able to stay afloat thanks to the insurance and continue investing into the ongoing research and development to impeccably perform future missions to protect society from serious and organized crime. In sum, insurance for unpreventable technical, operational, or legal risks will protect both sides of the table, making lawful hacking safer and more governable.

§ 4.3 Chapter Four Summary

This chapter comprehensively compiled a framework composed of the technical, operational, and legal findings on lawful hacking from the previous chapters of this dissertation. Chapter 4 eventually synthesized a multidisciplinary framework on lawful hacking composed of 15 interconnected and mutually supplementing sections. The primary purpose of this jurisdiction-neutral and technology-agnostic framework is to support lawmakers in making better-informed decisions when reviewing, enacting, or improving national legislation on lawful hacking, taking into consideration the privacy-protection needs, as well as the legitimate interests of justice to efficiently and effectively investigate and prosecute serious and organized crime. Additionally, the framework can help criminal defense lawyers, public prosecutors, and senior members of law enforcement agencies to better understand the crossdisciplinarity implications of cyber operations to make well-informed and better decisions. The framework is a systematically

structured embodiment of the principal work product created by this dissertation and the underlying research.

5. CHAPTER FIVE

§ 5.1 Research Findings

The first question of this research was formulated as follows: "What are the key technical obstacles and legal barriers that prevent law enforcement agencies from efficiently investigating serious criminal offenses without lawful hacking?" The short answer is: (i) the predominant availability of incriminating evidence solely in electronic form and format makes the physical search and seizure techniques inappropriate and requires deployment of digital forensics experts; (ii) the rapidly increasing misuse and exploitation of the technical progress by seasoned wrongdoers and transnational criminal syndicates, namely the misuse of strong encryption and other privacy-protection technologies available by default and at no additional cost, to prevent and obstruct traditional methods of digital forensics used within criminal investigations; (iii) the spiraling globalization of the Internet infrastructure that disperses incriminating digital evidence among numerous or even unknown foreign jurisdictions, with a heterogenous and incompatible legislation, and significantly delays and complexifies cross-border investigations and collaboration with foreign authorities and online services providers, to the extent that transborder digital investigations become futile; (iv) the raising global trend of strong privacy protection by design and by default that is leveraged as a strategic commercial advantage by online service providers and electronic device manufacturers, which vigorously resist collaborating with law enforcement agencies in criminal investigations; and (v) the now-obsolete legislation in relation to the lawful interception of electronic communications and other conventional investigation methods for telecommunication monitoring that became unavailing over a decade ago due to, inter alia, the omnipresent E2EE encryption, VoIP technologies, and other fruits of the technical

progress, which were unilaterally usurped and misappropriated by organized crime to cover and further their offenses. In sum, the efficient and effective investigation of serious and organized crime becomes virtually impossible without lawful hacking by police.

The second question of this research was formulated as follows: "How and to what extent can lawful hacking by law enforcement agencies be substituted by less intrusive means of investigations of technical or legal nature?" The short answer is: both technical and legal solutions of a less intrusive nature do exist and have been successfully used within criminal investigations, but all have a limited scope of practical applicability and thus cannot address the full spectrum of highly sophisticated and dangerous crimes, wherein seizure of electronic evidence may save lives, dismantle human trafficking, and expose multibillion fraud schemes with countless victims around the globe. Therefore, the available less-intrusive means of investigation require an enhancement with lawful hacking to successfully investigate and prosecute serious and organized crime.

The third question of this research was formulated as follows: "How can lawful hacking be regulated by national legislation to be efficient and to respect privacy and other individual rights, the integrity of criminal justice, and the rule of law?" The short answer is: by considering the 15 provisions of the jurisdiction-neutral framework produced in Chapter 4 of this research, lawmakers can implement or improve their national legislation on lawful hacking, which would reliably and overarchingly protect society, whilst in parallel stay operationally effective and cost-efficient in solving otherwise uninvestigable serious crimes. The same framework also may help judges, public prosecutors, criminal defense lawyers, and senior members of law enforcement agencies tasked with lawful hacking to better understand the multidisciplinary questions of cyber operations. In sum, by considering the framework, both the regulation of lawful hacking and its

practical implementation can properly balance the legitimate interests of criminal justice with privacy and other valuable human rights.

§ 5.2 Research Limitations

This research did not address classified cyber operations conducted by national intelligence or special military units, instead focusing on the lawful hacking conducted by police and other competent law enforcement agencies within criminal investigations under national criminal law. In continuation, the 15 provisions of the jurisdiction-neutral framework on lawful hacking available in Chapter 4, should not be interpreted as invariable, exhaustive, or absolute. Instead, the framework provisions serve as a lighthouse and reference point for sovereign states and their lawmakers seeking to enact or amend their national legislation on lawful hacking in a well-informed manner, taking into consideration the multidisciplinary aspects of contemporary cyber operations. That being said, the author of this framework hopes that this work can help both the opponents and proponents of lawful hacking to shape better arguments to cogently defend their opposing points of view, eventually synthesizing a privacy-friendly, technically effective, cost-effective, and sustainable legislation on lawful hacking that would allow law enforcement agencies to gradually suppress serious and organized crime, whilst duly protecting human rights and civil freedoms as much as possible. Likewise, the framework provisions are not intended to be incorporated into national legislation without a thoughtful consideration of country-specific legal, social, and cultural traditions, uniqueness of which must be unconditionally respected. Finally, despite the best efforts of the researcher to make the framework and its provisions as invulnerable to the impact of relentless technical progress and ongoing development of law, the 15 provisions of the framework should not be considered as permanently up-to-date and ought to be regarded through the prism of evolution.

§ 5.3 Contribution to the Body of Knowledge

This research utilized the general deterrence theory as a theoretical framework and conceptual prism to better understand, elaborate, and justify why lawful hacking by police —a heatedly debated topic at the time of writing—is both indispensable and socially desirable to investigate and prosecute serious and organized crime in a better and faster manner. The research demonstrated that less intrusive alternatives to lawful hacking—both of a technical and legal nature—do exist, however, they can only be practically applied under a narrow set of special circumstances and, therefore, cannot substitute lawful hacking to the extent necessary. The research then leveraged a multidisciplinary analysis and critical thinking to compile and synthesize the existing knowledge from the disciplines of computer science, law, and criminal justice to produce the actionable, jurisdiction-neutral, and technology-agnostic framework available in Chapter 4 of the research. The 15 mutually enhancing and mutually complementing provisions of the framework are designed to enable legal, judicial, and executive branches of governments from different countries around the globe to make well-informed and properly balanced decisions when enacting, amending, adjudicating, or enforcing their national legislation on lawful hacking. The underlying purpose of the produced framework is to build a solid interdisciplinary foundation and guidance for a holistic implementation of lawful hacking that would, on the one hand, overarchingly respect and safeguard privacy and other human rights and, on the other hand, enable law enforcement agencies to conduct technically effective and cost-efficient cyber operations against serious and organized crime, thereby saving taxpayers' money.

Prior to the publication of this research—which does not pretend to be pretend to be perfect or flawless—the available scholarly literature on lawful hacking was either narrowly

focused on one single discipline, for example, analyzing the implications of lawful hacking from a purely legal viewpoint and in isolation from the interrelated technical and operational context, or provided a cross-disciplinary but overly short and rather exploratory study of lawful hacking without offering an actionable solution to the existing problems. In a positive contrast, this dissertation and the underlying research successfully produced a multidisciplinary and comprehensive framework on lawful hacking with practical, actionable, and useful application to the real-world environment, expanding the existing body of knowledge.

§ 5.4 Recommendations for Future Research

The researcher proposes several ideas for upcoming research that may deserve the attention of legal or computer science scholars and doctoral researchers. First, a study that would suggest a specific cap on the scope, scale, and intrusiveness of lawful hacking—designed to avoid infringement of international law—would be invaluable for the sustainable development of the emerging body of national lawful on hacking legislation. Second, a study defining and clearly formulating the notification requirements owed to foreign states—impacted by lawful hacking operations—under international law would, likewise, bring the so-needed maturity and certainty to cross-border cyber operations conducted in the Internet by national law enforcement agencies. Third, an empirical study to compare the hacking methodologies and techniques of several law enforcement agencies from different countries and then benchmark the eventual success rate, time, and costs of operations classified by the underlying objectives and attack types would be immensely helpful in better prioritizing the efforts of police officers and focusing on the most technically effective and cost-efficient hacking techniques, specifically tailored for lawful hacking campaigns that differ from conventional penetration testing and ethical hacking. Fourth, a longitudinal study could assess whether investing in offensive cybersecurity training for law

enforcement officers economically outperforms the outsourcing of lawful hacking to third-party experts from private subcontractors, also focusing on talent acquisition costs before the training and talent retention costs after the training, helping to better understand the optimum allocation of police budgets. Fifth, a quantitative research, conducted through the lens of the general deterrence theory, could compare and correlate crime growth or decrease rates in jurisdictions with and without lawful hacking legislation, seeking a causal relationship between the two, whilst remaining mindful of the spurious relations of variables that could be caused by unknown, uncontrollable, or unconsidered external factors, as well as considering whether the would-be offenders are sufficiently informed about the legislation. Summarizing this section, the emerging sphere of lawful hacking certainly deserves further research by scholars from all disciplines.

§ 5.5 Research Recommendations

On the basis of multidisciplinary research and analysis, the researcher recommends that developed countries legalize lawful hacking by law enforcement agencies within investigations of serious or organized crime, without further delay. The legal vacuum in relation thereto is highly detrimental both to society and to criminal justice system. National legislation on lawful hacking should provide a reasonably broad and flexible investigatory cyber power to competent law enforcement agencies to attain the legitimate goals of justice, whilst in parallel imposing high standards of accountability and privacy protection on both police officers and prosecution in the execution of investigatory cyber operations. To facilitate and accelerate the lawmaking process, this research produced a jurisdiction-neutral and interdisciplinary framework composed of 15 mutually enhancing provisions, available in Chapter 4. Further delay in the implementation of national lawful hacking legislation, as well as the provision of law enforcement agencies with insufficient or overly restrictive investigation power in the cyberspace, will likely cause a rapid

proliferation of serious, transnational, and organized crime with almost absolute impunity, fostering unlawfulness on a global scale.

§ 5.6 About the Researcher

The researcher has over 15 years of practice in cybersecurity and cybercrime investigation. The researcher holds a Bachelor's degree in Computer Science (BSc) from Webster University, a Master's of Legal Studies (MLS) from Washington University in St. Louis, a Master's of Science (MSc) in Criminal Justice (Cybersecurity & Cybercrime Investigation) from Boston University, and a Master of Laws (LLM) in Information Technology Law from Edinburgh University.

§ 5.7 Chapter Five Summary

This chapter concluded the dissertation by concisely summarizing the findings and providing short answers to the three research questions. Then, Chapter 5 drew reader's attention to the research limitations related to practical implementation of the framework provided in the Chapter 4. Next, the chapter briefly elaborated on the contribution of this research to the existing body of knowledge, highlighting its practical application to solve important problems in the real-world environment. Additionally, this chapter suggested several currently unstudied areas of lawful hacking that may deserve further exploration and research. Finally, the chapter distilled brief recommendations based on the underlying research and its findings.

REFERENCES

Abel, W. (2010). Agents, Trojans and Tags: the Next Generation of Investigators. *International Review of Law, Computers & Technology, 23*(1-2), 99-108.

Abel, W., & Schafer, B. (2009). The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems - A Case Report on BVerfG, NJW 2008, 822. *SCRIPTed: A Journal of Law, Technology and Society, 6*(1), 106-123.

Acharya, B. (2021, April 27). Washington D.C. Police Server Hacked, Russian-Speaking Group Claims Responsibility. *Reuters*. Retrieved from https://www.reuters.com/world/europe/washington-dc-police-server-hacked-russian-speaking-group-claims-responsibility-2021-04-27/

Ahmed, J. U. (2010). Documentary Research Method: New Dimensions. *Indus Journal of Management & Social Sciences, 4*(1), 1-14.

Al-Sharif, Z., Bagci, H., Zaitoun, T., & Asad, A. (2018). Towards the Memory Forensics of MS Word Documents. In S. Latifi (Ed.), *Information Technology - New Generations. Advances in Intelligent Systems and Computing* (Vol. 558). Springer, Cham.

Anstis, S. (2021). Government Procurement Law and Hacking Technology: the Role of Public Contracting in Regulating an Invisible Market. *Computer Law & Security Review, 41*.

APA. (2020). *Publication Manual of the American Psychological Association (APA)* (7th ed.). Washington, DC: APA.

Apple. (2021). *CSAM Detection.* Apple Inc. Retrieved July 30, 2022, from https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf

Apple. (2022, May). *Apple Platform Security*. (Apple Inc.) Retrieved 30 2022, July , from https://support.apple.com/guide/security/welcome/web

Australian Department of Home Affairs. (2021, September 21). *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*. Retrieved from https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-act-2021

AWS. (2022). *AWS CloudHSM*. Retrieved July 30, 2022, from Amazon Web Services, Inc.: https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-toplevel.html

Baškarada, S. (2013). *Qualitative Case Study Guidelines.* Joint and Operations Analysis Division, Defence Science and Technology Organisation (DSTO). Retrieved July 30, 2022, from https://apps.dtic.mil/sti/pdfs/ADA594462.pdf

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report, 13*.

Beebe, B., Germano, R., Sprigman, C. J., & Steckel, J. H. (2019). Testing for Trademark Dilution in Court and the Lab. *University of Chicago Law Review, 86*(3), 611-668.

Bell, C. M. (2018). Surveillance Technology and Graymail in Domestic Criminal Prosecutions. *Georgetown Journal of Law & Public Policy, 16*(2), 537-558.

Bellovin, S. M. (2021, July-Aug). The Law and Lawful Hacking. *IEEE Security & Privacy, 19*, 76-76.

Bellovin, S. M., Blaze, M., & Landau, S. (2016). Insecure Surveillance: Technical Issues with Remote Computer Searches. *Computer, 49*(3), 14-24.

Bellovin, S. M., Blaze, M., Clark, S., & Landau, S. (2014). Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. *Northwestern Journal of Technology and Intellectual Property, 12*(1-2), 1-66.

Bellovin, S. M., Blaze, M., Landau, S., & Owsley, B. (2021). Seeking the Source: Criminal Defendants' Constitutional Right to Source Code. *Ohio State Technology Law Journal, 17*(1), 1-74.

Bercovitz, R. (2021). LAW ENFORCEMENT HACKING: DEFINING JURISDICTION. *Columbia Law Review, 121*(4), 1251-1288.

Bergman, R., & Kingsley, P. (2022, February 21). Israel Says Police Didn't Hack Civilians Without Court Approval. *The New York Times*. Retrieved from https://www.nytimes.com/2022/02/21/world/middleeast/israel-nso-spyware-investigation.html

Betschen, A. (2018). *Shining a Light on Federal Law Enforcement's Use of Computer Hacking Tools.* New York: Just Security, Reiss Center on Law and Security at New York University School of Law. Retrieved July 30, 2022, from https://www.justsecurity.org/60785/shining-light-federal-law-enforcements-computer-hacking-tools/

Bhattacherjee, A., & Shrivastava, U. (2018). The effects of ICT use and ICT Laws on corruption: A general deterrence theory perspective. *Government Information Quarterly, 35*, 703-712.

Bhuiyan, J. (2021, March 24). This Is What Happens When ICE Asks Google for Your User Information. *Los Angelos Times*. Retrieved from https://www.latimes.com/business/technology/story/2021-03-24/federal-agencies-subpoena-google-personal-information

Blažič, B. J., & Klobučar, T. (2020). Removing the Barriers in Cross-Border Crime Investigation by Gathering e-Evidence in an Interconnected Society. *Information & Communications Technology Law*(1), 66-81.

Blue, V. (2014, August 6). Top Gov't Spyware Company Hacked; Gamma's FinFisher Leaked. *ZDNet*. Retrieved July 30, 2022, from https://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked/

Bouchaud, F., Vantroys, T., & Grimaud, G. (2021). Evidence Gathering in IoT Criminal Investigation. In S. Goel, P. Gladyshev, D. Johnson, M. Pourzandi, & S. Majumdar (Eds.), *Digital Forensics and Cyber Crime. ICDF2C 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* (Vol. 351). Cham: Springer.

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal, 9*(2), 27-40.

Bowles, S., & Hernandez-Castro, J. (2015). The First 10 Years of the Trojan Horse Defence. *Computer Fraud & Security, 2015*(1), 5-13.

Brandao, P. R. (2019). Forensics and Digital Criminal Investigation Challenges in Cloud Computing and Virtualization. *American Journal of Networks and Communications, 8*(1), 23-31.

Brown, S. D. (2020). Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice. *ERA Forum 20, 423–438*.

Bullock, D., Aliyu, A., Maglaras, L., & Ferrag, M. A. (2020). Security and Privacy Challenges in the Field of iOS Device Forensics. *AIMS Electronics and Electrical Engineering, 4*(3), 249–258.

Bureau of Justice Assistance. (2022). *Electronic Communications Privacy Act of 1986 (ECPA).* The Bureau of Justice Assistance (US). Retrieved July 30, 2022, from https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

Burns, A. J., Johnson, E., & Caputo, D. D. (2019). Spear Phishing in a Barrel: Insights From a Targeted Phishing Campaign. *Journal of Organizational Computing and Electronic Commerce, 29*(1), 24-39.

Cahyani, N. D., Rahman, N., Xu, Z., Glisson, W., & Choo, K.-K. (2016). The Role of Mobile Forensics in Terrorism Investigations Involving the Use of Cloud Apps. *MobiMedia '16: Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, 199–204.

California Office of the Attorney General. (2022). *Communication Service Providers Legal Process Information.* State of California Department of Justice. Retrieved July 30, 2022, from https://oag.ca.gov/ecrime/csp-reporting

Caproni, V. (2011, February 11). *Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security*. Retrieved from FBI: https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

Carter, W. A. (2019). *Ensuring Data Security Against Lawful and Unlawful Threats in the Digital Age.* Washington, DC: Center for Strategic & International Studies (CSIS). Retrieved July 30, 2022, from https://www.judiciary.senate.gov/download/carter-testimony

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border Criminal Investigations and Digital Evidence. doi:https://doi.org/10.48550/arXiv.2205.12911

Cellbrite. (2019, January 8). *How Wearables Are Being Used to Solve Homicides, Missing Person and Illicit Drug Cases*. Retrieved from https://cellebrite.com/en/how-wearables-are-being-used-to-solve-homicides-missing-person-and-illicit-drug-cases/

CEPOL. (2021). *European Union Strategic Training Needs Assessment 2022-2025.* Budapest: The European Union Agency for Law Enforcement Training (CEPOL). Retrieved July 30, 2022, from https://www.cepol.europa.eu/sites/default/files/EU-STNA-2022-CEPOL.pdf

CEPOL. (2022). *Digital Forensics Training.* Retrieved July 30, 2022, from https://www.cepol.europa.eu/tags/digital-forensics

Chauriye, N. (2016). Wearable Devices as Admissible Evidence: Technology is Killing. *Catholic University of America, Columbus School of Law, 24*(2). Retrieved from https://scholarship.law.edu/jlt/vol24/iss2/9

Cheung, A. K. (2014). Structured Questionnaires. In A. C. Michalos (Ed.), *Encyclopedia of Quality of Life and Well-Being Research.* Dordrecht: Springer.

Claburn, T. (2022, August 4). One to Watch: Open-Source Code That Measures Our Exposure to CCTV. *The Register*. Retrieved August 15, 2022, from https://www.theregister.com/2022/08/04/cctv_exposure_tool/

Cochrane, T. (2021). Hiding in the Eye of the Storm Cloud: How Cloud Act Agreements Expand U.S. Extraterritorial Investigatory Powers. *Duke Journal of Comparative and International Law, 32*(1), 153-210.

Comey, J. B. (2014, October 16). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* Retrieved from FBI: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Committee on Counter-Terrorism [CDCT]. (2021). *Profiles on Counter-Terrorism Capacity: France.* Strasbourg : The Council of Europe (CoE) Committee on Counter-Terrorism (CDCT). Retrieved July 30, 2022, from https://rm.coe.int/profile-france-2021-cdct-/1680a44e0c

Council of Europe. (2022). *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY.* Retrieved July 30, 2022, from https://www.coe.int/en/web/cybercrime/parties-observers

Council of Europe. (2022a). *Enhanced Co-Operation and Disclosure of Electronic Evidence: 22 Countries Sign New Protocol to Cybercrime Convention.* Strasbourg: Council of Europe. Retrieved July 30, 2022, from https://www.coe.int/en/web/portal/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention

Cox, J. (2017, January 12). Hacker Steals 900 GB of Cellebrite Data. *VICE*. Retrieved July 30, 2022, from https://www.vice.com/en/article/3daywj/hacker-steals-900-gb-of-cellebrite-data

Cox, J. (2022, June 3). A European Country Helped the FBI Intercept Anom Messages, But It Wants to Remain Hidden. *VICE*. Retrieved July 30, 2022, from https://www.vice.com/en/article/qjbggq/anom-third-country-europe-european-union-fbi

Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications .

Crist, R. (2022, July 26). Ring, Google and the Police: What to Know About Emergency Requests for Video Footage. *CNET*. Retrieved July 30, 2022, from

https://www.cnet.com/home/security/ring-google-and-the-police-what-to-know-about-emergency-requests-for-video-footage/

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The Case Study Approach. *BMC Medical Research Methodology, 11*(100).

Crown Prosecution Service. (2022, July 14). *Disclosure Manual: Chapter 30 - Digital Material*. Retrieved from The UK Crown Prosecution Service: https://www.cps.gov.uk/legal-guidance/disclosure-manual-chapter-30-digital-material

Culafi, A. (2020, June 16). CIA Unaware of Vault 7 Theft Until WikiLeaks Dump. *TechTarget*. Retrieved July 30, 2020, from https://www.techtarget.com/searchsecurity/news/252484761/CIA-unaware-of-Vault-7-theft-until-WikiLeaks-dump

Cummins Flory, T. (2016). Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana. *Journal of Digital Forensics, Security and Law, 11*(1), Article 4.

Cuthbertson, A. (2018, August 31). How Not Sharing Your Facebook Password Could Lead to Prison. *The Independent*. Retrieved July 30, 2022, from https://www.independent.co.uk/tech/facebook-password-ripa-law-prison-lucy-mchugh-a8517176.html

Cybersecurity and Infrastructure Security Agency. (2020). *Avoiding Social Engineering and Phishing Attacks.* Cybersecurity and Infrastructure Security Agency (CISA). Retrieved July 30, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST04-014

Cybersecurity and Infrastructure Security Agency. (2021). *Top Routinely Exploited Vulnerabilities.* US Cybersecurity and Infrastructure Security Agency (CISA). Retrieved July 30, 2022, from https://www.cisa.gov/uscert/ncas/alerts/aa21-209a

Cybersecurity and Infrastructure Security Agency. (2022). *Preparing Critical Infrastructure for Post-Quantum Cryptography.* Washington D.C.: The US Cybersecurity and Infrastructure Security Agency (CISA). Retrieved August 28, 2022, from https://cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf

Cyphers, B., & Gebhart, G. (2019). *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance.* The Electronic Frontier Foundation (EFF). Retrieved from https://www.eff.org/wp/behind-the-one-way-mirror

Darke, P., & Shanks, G. (2002). *Topics in Australasian Library and Information Studies, Research Methods for Students, Academics and Professionals* (Second ed.). Chandos Publishing.

Daskal, J. (2019). Unpacking the CLOUD Act. *eucrim*, 220-225.

Daskal, J. C. (2020). Transnational Government Hacking. *Joint PIJIP/TLS Research Paper Series, 52*.

Daskal, J., & Kennedy-Mayo, D. (2020). *Budapest Convention: What is it and How is it Being Updated?* Cross-Border Data Forum. Retrieved July 30, 2022, from https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/

Davies, G. (2020). Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers. *The Journal of Criminal Law, 84*(5), 407-426.

De Bolle, C., & Vance, C. R. (2021, July 26). The Last Refuge of the Criminal: Encrypted Smartphones. *Politico*. Retrieved July 30, 2022, from https://www.politico.eu/article/the-last-refuge-of-the-criminal-encrypted-smartphones-data-privacy/

Dees, T. (2018, January 29). How Police Can Obtain Evidence From the Cloud. *Police1*. Retrieved July 30, 2022, from https://www.police1.com/police-products/investigation/computer-digital-forensics/articles/how-police-can-obtain-evidence-from-the-cloud-X2bX137fJVI5NefK/

Delerue, F. (2020). *Cyber Operations and International LAw.* Cambridge: Cambridge University Press.

Department of Justice. (2020). *International Statement: End-To-End Encryption and Public Safety* . Washington, DC: The US Department of Justice, Office of Public Affairs. Retrieved from https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

Department of Justice. (2022). *Cloud Act Resources.* Washington D.C.: The US Department of Justice, the Computer Crime and Intellectual Property Section (CCIPS). Retrieved July 30, 2022, from https://www.justice.gov/dag/cloudact

Dickson, B. (2021, September 21). What is Steganography? A Complete Guide to the Ancient Art of Concealing Messages. *The Daily Swig*. Retrieved July 30, 2022, from https://portswigger.net/daily-swig/what-is-steganography-a-complete-guide-to-the-ancient-art-of-concealing-messages

Dizon, M. A., & Upson, P. J. (2021). Laws of Encryption: an Emerging Legal Framework. *Computer Law & Security Review, 43*.

EastWest Institute. (2018). *Encryption Policy in Democratic Regimes, Finding Convergent Paths and Balanced Solutions.* New York: The EastWest Institute. Retrieved July 30, 2022, from https://www.eastwest.ngo/sites/default/files/ewi-encryption.pdf

Edmonson, A. (2021). Password Unprotected: Compelled Disclosure of Cellphone. *Rutgers Computer and Technology Law, 48*(1), 117-146.

EDPB & EDPS. (2019). *EDPB-EDPS Joint Response to the LIBE Committee on the Impact of the US Cloud Act on the European Legal Framework for Personal Data Protection.* Retrieved July 30, 2022, from https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en

EDPB & EDPS. (2022). *Proposal to Combat Child Sexual Abuse Online Presents Serious Risks for Fundamental Rights.* Brussels: The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS). Retrieved July 30, 2022, from https://edpb.europa.eu/news/news/2022/proposal-combat-child-sexual-abuse-online-presents-serious-risks-fundamental-rights_nl

Electronic Privacy Information Center [EPIC]. (2014). *Concerning the Constitutionality of a Warrantless Cell Phone Search Incident to Arrest.* Washington, DC: Electronic Privacy Information Center. Retrieved July 30, 2022, from https://epic.org/documents/riley-v-california-2/

ENISA. (2019). *Encrypted Traffic Analysis: Use Cases & Security Challanges.* The European Union Agency for Cybersecurity. Retrieved July 30, 2022, from https://www.enisa.europa.eu/publications/encrypted-traffic-analysis/at_download/fullReport

EU SIRIUS. (2021). *3rd Annual SIRIUS EU Digital Evidence Report.* European Union Agency for Law Enforcement Cooperation. Retrieved July 30, 2022, from https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_DESR_12_2021.pdf

European Commission. (2018). *New EU rules to obtain electronic evidence.* The European Commission . Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

European Commission. (2018). *Proposal for a European Production and Preservation Orders for Electronic Evidence in Criminal Matters.* Strasbourg: European Commission. Retrieved July 30, 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225

European Data Protection Board. (2021). *Statement 02/2021 on New Draft Provisions of the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention).* The European Data Protection Board. Retrieved July 30, 2022, from https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_en

European Digital Rights. (2021). *Demonstrating Gaps in the E-Evidence Regulation.* European Digital Rights association. Retrieved July 30, 2022, from https://edri.org/wp-content/uploads/2021/10/EDRI_eEvidence.pdf

European Judicial Network [EJN]. (2020). *Fiches Belges on Electronic Evidence: France.* The European Judicial Network (EJN). Retrieved July 30, 2022, from https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/France_Fiches%20Belges-on-electronic-evidence.pdf

European Telecommunications Standards Institute. (2021). *Lawful Interception (LI): Requirements of Law Enforcement Agencies.* Sophia Antipolis: The European Telecommunications Standards Institute (ETSI). Retrieved July 30, 2022, from

https://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.07.01_60/ts_101331v010701p.pdf

Europol & ENISA. (2016). *On Lawful Criminal Investigation That Respects 21st Century Data Protection.* Retrieved July 30, 2022, from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

Europol & Eurojust. (2019). *First joint report of the observatory function on encryption.* Hague. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/final_report_of_the_observatory_function.pdf

Europol & Eurojust. (2021). *Third Report of the Observatory Function on Encryption.* Europol and Eurojust. Retrieved July 30, 2022, from https://www.eurojust.europa.eu/sites/default/files/assets/joint-ep-ej-third-report-of-the-observatory-function-on-encryption-en.pdf

Europol. (2016). *Internet Organized Crime Threat Assessment (IOCTA).* The Hague. Retrieved July 30, 2022, from https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf

Europol. (2020). *Europol and the European Commission Inaugurate New Decryption Platform to Tackle the Challenge of Encrypted Material for Law Enforcement Investigations.* The Hague: Europol. Retrieved July 30, 2022, from https://www.europol.europa.eu/media-press/newsroom/news/europol-and-european-commission-inaugurate-new-decryption-platform-to-tackle-challenge-of-encrypted-material-for-law-enforcement

Europol. (2021). *European Union Serious and Organised Crime Threat Assessment (EU SOCTA) 2021.* The Hagues: Europol. Retrieved July 30, 2022, from https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

Europol. (2021a). *800 Criminals Arrested in Biggest Ever Law Enforcement Operation Against Encrypted Communication.* The Hague: Europol. Retrieved July 30, 2022, from https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

Farlow, H., & Edwards, B. M. (2022). Shining a Light on 'Going Dark': a Framework to Guide the Co-Design and Communication of Decryption Laws Based on the Passage of the Telecommunications and Other Legislation (Assistance and Access) Bill 2018. *Computer Law & Security Review, 46*.

Fernandes, R., Colaco, R. M., Shetty, S., & Moor, R. (2020). A New Era of Digital Forensics in the form of Cloud Forensics: A Review. *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 422-427). Coimbatore: IEEE.

Fernández-Álvarez, P., & Rodríguez, R. J. (2022). Extraction and Analysis of Retrievable Memory Artifacts From Windows Telegram Desktop Application. *Forensic Science International: Digital Investigation, 40, Supplement*.

Fidler, M. (2020). Local Police Surveillance and the Administrative Fourth Amendment. *Santa Clara High Technology Law Journal, 36*(5), 481-561.

Forrest, M. (2022, July 26). Canadian Parliament to Probe Police Use of Spyware. *POLITICO*. Retrieved July 30, 2022, from https://www.politico.com/news/2022/07/26/canadian-parliamentarians-police-use-spyware-00048044

Freet, D., Agrawal, R., John, S., & Walker, J. J. (2015). Cloud Forensics Challenges From a Service Model Standpoint: IaaS, PaaS and SaaS. *Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems (MEDES '15)* (pp. 148-155). New York: Association for Computing Machinery.

Freiling, F., & Hösch, L. (2018). Controlled Experiments in Digital Evidence Tampering. *Digital Investigation, 24*(Supplement), S83-S92.

Fukami, A., Stoykova, R., & Geradts, Z. (2021). A New Model for Forensic Data Extraction From Encrypted Mobile Devices. *Forensic Science International: Digital Investigation, 38*.

Garcha, R. K. (2018). Nits a No-Go: Disclosing Exploits and Technological Vulnerabilities in Criminal Cases. *New York University Law Review, 93*(4), 822-863.

Ghafarian, A., & Wood, C. (2019). Forensics Data Recovery of Skype Communication from Physical Memory. In K. Arai, S. Kapoor, & R. Bhatia (Eds.), *Advances in Intelligent Systems and Computing.* NameSpringer, Cham.

Ghappour, A. (2017). Searching Places Unknown: Law Enforcement Jurisdiction on the Dark. *Stanford Law Review, 69*(4), 1075-1136.

Gibbs, J. P. (1985). Deterrence Theory and Research. *Nebraska Symposium on Motivation, 33*.

Goodwin, B. (2022, March 11). Police EncroChat Cryptophone Hacking Implant Did Not Work Properly and Frequently Failed. *ComputerWeekly*. Retrieved July 30, 2022, from https://www.computerweekly.com/news/252514476/Police-EncroChat-cryptophone-hacking-implant-did-not-work-properly-and-frequently-failed

Gozman, D., & Willcocks, L. (2019). The emerging Cloud Dilemma: Balancing Innovation with Cross-Border Privacy and Outsourcing Regulations. *Journal of Business Research, 97*, 235-256.

Granick, J. S. (2017). *Challenging Government Hacking: What's at Stake.* American Civil Liberties Union (AUCLA). Retrieved July 30, 2022, from https://www.aclu.org/blog/privacy-technology/internet-privacy/challenging-government-hacking-whats-stake

Greenberg, A. (2015, January 13). Silk Road Defense Says Ulbricht Was Framed by the 'Real' Dread Pirate Roberts. *WIRED*. Retrieved July 30, 2022, from https://www.wired.com/2015/01/isilk-road-trial-opening-statements/

Greenberg, A. (2022, June 16). Police Linked to Hacking Campaign to Frame Indian Activists. *WIRED*. Retrieved from https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/

Gutheil, M., Liger, Q., Heetman, A., Eager, J., & Crawford, M. (2017). *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices.* Brussels: The European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs. Retrieved July 30, 2022, from https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

Haselton, T. (2018, August 20). How to Send Self-Destructing Emails in Gmail. *CNBC*. Retrieved from https://www.cnbc.com/2018/08/20/how-to-send-self-destructing-email-gmail-confidential-mode.html

Hausknecht, K., Foit, D., & Burić, J. (2015). RAM data significance in digital forensics. *38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1372-1375.

Hayes, R., Kyer, B., & Weber, E. (2015). *The case study cookbook.* Worcester, MA: Worcester Polytechnic Institute.

Hennessey, S. (2016, Apil 21). Encryption Legislation: Critics Blinded by Outrage are Blinded to the Lessons. *The Lawfare Institute*. Retrieved July 30, 2022, from https://www.lawfareblog.com/encryption-legislation-critics-blinded-outrage-are-blinded-lessons

Herpig, S. (2018). *A Framework for Government Hacking in Criminal Investigations.* Stiftung Neue Verantwortung. Retrieved July 30, 2022, from https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf

Herrera, L. A. (2020). Challenges of Acquiring Mobile Devices While Minimizing the Loss of Usable Forensics Data. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1-5.

Hewson, E. C., & Harrison, P. (2021). Talking in the Dark: Rules to Facilitate Open Debate About Lawful Access to Strongly Encrypted Information. *Computer Law & Security Review, 40*.

Hill, D. J., McLeod, S. K., & Tanyi, A. (2018). The Concept of Entrapment. *Criminal Law and Philosophy, 12*, 539–554.

Hill-Smith, M. (2019). Smartphone Encryption: a Legal Framework for Law Enforcement to Survive the "Going Dark" Phenomenon. *Auckland University Law Review, 25*, 173-198.

Hope, A. (2022, June 22). Over 24 Billion Compromised User Credentials Circulating on the Dark Web Market. *CPO Magazine*. Retrieved July 30, 2022, from https://www.cpomagazine.com/cyber-security/over-24-billion-compromised-user-credentials-circulating-on-the-dark-web-market/

Humphries, G., Nordvik, R., Manifavas, H., Cobley, P., & Sorell, M. (2021). Law Enforcement Educational Challenges for Mobile Forensics. *Forensic Science International: Digital Investigation, 38, Supplement*.

Institute for Human Rights and Business. (2016). *Designing a Legal Regime for Lawful Interception and Government Access to User Data.* London: Institute for Human Rights and Business (IHRB). Retrieved July 30, 2022, from https://www.ihrb.org/uploads/reports/2016-1-15_Lawful_Interception_Government_Access_User_Data.pdf

International Association of Chiefs of Police. (2015). *A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence.* Alexandria, VA: The International Association of Chiefs of Police (IACP). Retrieved July 30, 2022, from https://www.theiacp.org/sites/default/files/2019-05/IACPSummitReportGoingDark_0.pdf

Internet Society. (2020). *Fact Sheet: Government Hacking.* Geneva: The Internet Society. Retrieved July 30, 2022, from https://www.internetsociety.org/resources/doc/2020/fact-sheet-government-hacking/

INTERPOL. (2019). *Global Guidelines for Digital Forensics Labarotories.* Retrieved from https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

INTERPOL. (2021). *INTERPOL Global Horizon Scan.* INTERPOL Innovation Centre. Retrieved July 30, 2022, from https://www.interpol.int/es/content/download/17281/file/IC_07%20Policing%20Futures%20November%202021.pdf

Janarthanan, T., Bagheri, M., & Zargari, S. (2021). IoT Forensics: An Overview of the Current Issues and Challenges. In R. Montasari, H. Jahankhani, R. Hill, & S. Parkinson (Eds.), *Digital Forensic Investigation of Internet of Things (IoT) Devices. Advanced Sciences and Technologies for Security Applications.* Cham: Springer.

Janesick, V. J. (2015). Peer Debriefing. In G. Ritzer (Ed.), *The Blackwell Encyclopedia of Sociology.*

Jarrett, H. M., Bailie, M. W., Hagen, E., & Judish, N. (2009). *Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* The US Department of Justice, Computer Crime and Intellectual Property Section Criminal Division. Office of Legal Education Executive Office for United States Attorneys. Retrieved July 30, 2022, from https://www.justice.gov/file/442111/download

Jayapaul, R. (2021). *Telegram Self-Destruct? Not Always.* Trustwave Holdings, Inc. Retrieved July 30, 2022, from https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/telegram-self-destruct-not-always/

Johnson, B. (2019). *Do Criminal Laws Deter Crime? Deterrence Theory in Criminal Justice Policy: A Primer.* Minnesota Legislature - Minnesota House of Representatives - House Research. Retrieved July 30, 2022, from https://www.lrl.mn.gov/docs/2019/other/190398.pdf

Jones, T. (2021, June 29). A Cloud Services Cheat Sheet for AWS, Azure and Google Cloud. *TechTarget*. Retrieved from https://www.techtarget.com/searchcloudcomputing/feature/A-cloud-services-cheat-sheet-for-AWS-Azure-and-Google-Cloud

Kargopoulos, A.-I. (2021). *Challenges of Implementing Procedural Law From the Perspective of Fundamental Rights Safeguards and Guarantees.* The European Union Agency for Fundamental Rights. Retrieved July 30, 2021, from https://rm.coe.int/ws5-5-challenges-of-implementing-procedural-law-from-the-perspective-o/1680a49000

Keenan, B. (2019). State Access to Encrypted Data in the United Kingdom: the 'Transparent' Approach. *Common Law World Review, 49*(3-4), 223-244.

Kerr, O. (2018, June 26). Does Carpenter Revolutionize the Law of Subpoenas? *Lawfare*. Retrieved from https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas

Kerr, O. (2021). 'Decryption Originalism: the Lessons of Burr'. *Harvard Law, 134*(3), 905-963.

Kleijssen, J., & Perri, P. (2017). Cybercrime, Evidence and Territoriality: Issues and Options. In *In: Kuijer, M., Werner, W. (eds) Netherlands Yearbook of International Law 2016* (p. 149). The Hague: Netherlands Yearbook of International Law, vol 47. T.M.C. Asser Press.

Kolb, B. (2007). Les Nouvelles Technologies de l'Information et de la Communication, Vers une Surdité Annoncée de nos Autorités d'Enquête Pénale. *Master Thesis Publication (French) (Unpublished)*. Retrieved July 30 2022

Koops, B.-J., & Kosta, E. (2018). Looking for Some Light Through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities Against "Going Dark". *Computer Law & Security Review, 34*, 890-900.

Kortmann, F. (2020). *Police Hacking in the Netherlands.* Tilburg: Master Thesis Law & Technology, Tilburg University, SNR 2046839.

Kovacs, E. (2016, Junuary 5). Dutch Government Opposes Encryption Backdoors. *SecurityWeek*. Retrieved July 30, 2022, from https://www.securityweek.com/dutch-government-opposes-encryption-backdoors

Kovacs, E. (2020, June 24). Twitter Suspends Account of Organization Behind Police Leaks. *SecurityWeek*. Retrieved July 30, 2022, from https://www.securityweek.com/twitter-suspends-account-organization-behind-police-leaks

Krebs, B. (2022, March 29). *Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"*. Retrieved from Krebs on Security : https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests/

Kumar, S. (2022). *How Can Digital Rights Defenders Respond to the Rising Use of Government Hacking as the Internet of Things Grows?* Amsterdam: Digital Freedom Fund. Retrieved July 30, 2022, from https://digitalfreedomfund.org/how-can-digital-rights-defenders-respond-to-the-rising-use-of-government-hacking-as-the-internet-of-things-grows/

Lawal, D. O., Gresty, D. W., Gan, D. E., & Hewitt, L. (2021). Have You Been Framed and Can You Prove It? *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)*, 1236-1241.

Leyden, J. (2007, November 21). Germany Seeks Malware 'Specialists' to Bug Terrorists. *The Register*. Retrieved July 30, 2022, from https://www.theregister.com/2007/11/21/germany_vxer_hire_plan/

Li, C.-Y., Huang, C.-C., Lai, F., Lee, S.-L., & Wu, J. (2018). A Comprehensive Overview of Government. *IEEE Access, 6*, 55053-55073.

Li, X., & Qin, Y. (2018). Research on Criminal Jurisdiction of Computer Cybercrime. *Procedia Computer Science, 131*, 793-799.

Liguori, C. (2020). Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate. *Michigan Technology Law Review, 26*(2), 317-346.

Lindemann, M., & van Toor, D. (2018, May). Protection of a Suspect's Privacy in Criminal Procedure. *Ars Aequi*, 376-384.

Lindenlauf, S., Höfken, H., & Schuba, M. (2015). Cold Boot Attacks on DDR2 and DDR3 SDRAM. *2015 10th International Conference on Availability, Reliability and Security*, 287-292.

Liptak, A. (2018, June 22). In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy. *The New York Times*. Retrieved July 30, 2022, from https://www.nytimes.com/2018/06/22/us/politics/supreme-court-warrants-cell-phone-privacy.html

Lomas, N. (2016, March 10). UK Surveillance Powers Bill Could Force Startups to Bake in Backdoors. *TechCrunch*. Retrieved July 30, 2022, from https://techcrunch.com/2016/03/10/uk-surveillance-powers-bill-could-force-startups-to-bake-in-backdoors/

Lowe, D. (2021). Post-Brexit will EU Data Protection Law Still Impact on Police Investigations into Terrorism and Organised Crime? *Expert Witness Journal*.

Lutta, P., Sedky , M., Hassan, M., Jayawickrama, U., & Bastaki, B. B. (2021). The Complexity of Internet of Things Forensics: a state-of-the-Art Review. *Forensic Science International: Digital Investigation, 38*.

Lyle, J. R., Guttman, B., Butler, J. M., Sauerwein, K., Reed, C., & Lloyd, C. E. (2022). *Digital Investigation Techniques: A NIST Scientific Foundation Review (NISTIR 8354-DRAFT).* Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354-draft.pdf

Lynch, J. (2011). *New FBI Documents Provide Details on Government's Surveillance Spyware.* The Electronic Frontier Foundation. Retrieved July 30, 2022, from https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government

MacDermott, A., Baker, T., & Shi, Q. (2018). Iot Forensics: Challenges for the Ioa Era. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1-5.

Maimon, D. (2020). Deterrence in Cyberspace: An Interdisciplinary Review of the Empirical Literatur. In T. J. Holt, & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. pp 449-467). Palgrave Macmillan, Cham.

Majed, H., Noura, H. N., & Chehab, A. (2020). Overview of Digital Forensics and Anti-Forensics Techniques. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1-5.

Mambodza, W. T., & NagoorMeeran, A. (2015). Android Mobile Forensic Analyzer for Stegno Data. *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, 1-8.

Manral, B., Somani, G., Choo, K.-K. R., Conti, M., & Gaur, M. S. (2019). A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions. *ACM Computing Surveys (CSUR), 52*(6), 1-38.

Mateusz Stępień. (2019). Using Case Studies for Research on Judicial Opinions. Some Preliminary Insights. *Law and Method*.

May, C. (2021, January 13). *Conducting a Digital Forensics Capability Study*. Retrieved from FBI: https://leb.fbi.gov/articles/featured-articles/conducting-a-digital-forensics-capability-study

Mayer, J. (2018). Government Hacking. *The Yale Law Journal, 127*(3), 570–662.

McMillan, J. E., Glisson, W. B., & Bromby, M. (2013). Investigating the Increase in Mobile Phone Evidence in Criminal Activities. *2013 46th Hawaii International Conference on System Sciences*, 4900-4909.

Megret, F. (2020). Do Not Do Abroad What You Would Not Do at Home? *Canadian Yearbook of International Law/Annuaire Canadien De Droit International*, 1-40.

Menn, J. (2020, January 21). Exclusive: Apple Dropped Plan for Encrypting Backups After FBI Complained. *Reuters*. Retrieved July 30, 2022, from https://www.reuters.com/article/us-apple-fbi-icloud-exclusive-idUSKBN1ZK1CT

Merken, S. (2021, May 17). U.S. Supreme Court Nixes Appeal Over Forced Password Disclosure. *Reuters*. Retrieved July 30, 2022, from https://www.reuters.com/business/legal/us-supreme-court-nixes-appeal-over-forced-password-disclosure-2021-05-17/

Microsoft. (2021). *Law Enforcement Requests Report.* Retrieved July 30, 2022, from https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

Mistry, N., Christian, A., & Bhavsar, B. (2020). Volatile Memory Disk Forensics: Investigate the Criminal Activity of RAMDisk. In M. Tuba, S. Akashe, & A. Joshi (Eds.), *ICT Systems*

and Sustainability. Advances in Intelligent Systems and Computing, (Vol. 1270). Singapore: Springer.

Moloney, C. J., Unnithan, N., & Zhang, W. (2022). *Assessing Law Enforcement's Cybercrime Capacity and Capability.* FBI, Law Enfrocement Bulletin. Retrieved July 30, 2022, from https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability-

Momsen, C. (2022). Relevance of Data Security and Data Protection in Companies from the Perspective of Criminal Law. In *Handbook Industry 4.0.* (Walter Frenz ed., pp. 42-69). Berlin: Springer.

Monshizadeh, M., Khatri, V., Varfan, M., & Kantola, R. (2018). LiaaS: Lawful Interception as a Service. *26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*.

Moraes, T. (2020). Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures. *European Data Protection Law Review (EDPL), 6*(1), 41-55.

Morris, N. (2009, Junuary 5). New Powers for Police to Hack Your PC. *The Independent*. Retrieved July 30, 2022, from https://www.independent.co.uk/tech/new-powers-for-police-to-hack-your-pc-1225802.html

Mullin, J. (2022). *The EU Commission's New Proposal Would Undermine Encryption And Scan Our Messages.* The Electronic Frontier Foundation. Retrieved July 30, 2022, from https://www.eff.org/deeplinks/2022/05/eu-commissions-new-proposal-would-undermine-encryption-and-scan-our-messages

Murphy, C. C. (2020). The Crypto-Wars Myth: the Reality of State Access to Encrypted Communications. *Common Law World Review, 49(3–4)*, 245–261.

Nakashima, E., & Albergotti, R. (2021, april 14). The FBI Wanted to Unlock the San Bernardino Shooter's iPhone. It Turned to a Little-Known Australian Firm. *The Washington Post*. Retrieved July 30, 2022, from https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/

Napoleon, P., Saturnia, O., Shoesmith, M., & Petrovitch, J. (2021). *The Use of Encrypted Communications by Criminals.* The Counterterrorism Group, Inc. Retrieved July 30, 2022, from https://www.counterterrorismgroup.com/post/the-use-of-encrypted-communications-by-criminals

National Consortium for Justice Information and Statistics. (2022). *ISP List and LE Guides.* The National Consortium for Justice Information and Statistics (SEARCH). Retrieved July 30, 2022, from https://www.search.org/resources/isp-list/

National Institute of Justice. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* Retrieved from https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

National Institute of Justice. (2020). *Digital Evidence Policies and Procedures Manual*. Retrieved from The US National Institute of Justice (NIJ): https://nij.ojp.gov/library/publications/digital-evidence-policies-and-procedures-manual

National Institute of Justice. (2022). *Digital Evidence and Forensics.* Retrieved July 30, 2022, from https://nij.ojp.gov/digital-evidence-and-forensics

National Institute of Standards and Technology. (2022). *Digital Evidence*. Retrieved July 30, 2022, from The National Institute of Standards and Technology (NIST): https://www.nist.gov/digital-evidence

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Communications Surveys & Tutorials, 21*(3), 2702-2733.

Nichols, S. (2021, August 11). Hackers selling access to breached networks for $10,000. *TechTarget*. Retrieved from https://www.techtarget.com/searchsecurity/news/252505163/Hackers-selling-access-to-breached-networks-for-10000

Nield, D. (2022, June 27). 7 Apps That Will Let You Send Disappearing Messages. *Popular Science*. Retrieved July 2022, 30, from https://www.popsci.com/send-self-destructing-messages/

NIST. (2019). *Computer Forensics Tool Testing Program (CFTT).* Retrieved from https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

OFAC. (2021). *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments.* Washington, DC: US Department of the Treasury, Office of Foreign Assets Control (OFAC). Retrieved July 30, 2022, from https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

Office of Justice Programs [OJP]. (2003). *Obtaining Admissible Evidence From Computers and Internet Service Providers.* The US Office of Justice Programs. Retrieved from

https://www.ojp.gov/ncjrs/virtual-library/abstracts/obtaining-admissible-evidence-computers-and-internet-service

Ohm, P. (2017). The Investigative Dynamics of the Use of Malware by Law Enforcement. *William & Mary Bill of Rights Journal, 26*(2), 303-336.

OLAF. (2016). *Guidelines on Digital Forensic Procedures for OLAF Staff.* Retrieved from https://anti-fraud.ec.europa.eu/investigations/digital-forensics_en

Olber, P. (2021). The Survey on Cross-Border Collection of Digital Evidence by Representatives from Polish Prosecutors' Offices and Judicial Authorities. *Journal of Digital Forensics, Security and Law, 16*, Article 3.

Ölvecký, M., & Gabriska, D. (2018). Wiping Techniques and Anti-Forensics Methods. *IEEE 16th International Symposium on Intelligent Systems and Informatics.* Subotica.

O'Neill, P. H. (2019, November 29). The Fall and Rise of a Spyware Empire. *MIT Technology Review*. Retrieved July 30, 2022, from https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of Things Forensics: Challenges and approaches. *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing* (pp. 608-615). Austin: IEEE.

Osula, A.-M. (2015). Transborder Access and Territorial Sovereignty. *Computer Law & Security Review*, 719-735.

Osula, A.-M., & Zoetekouw, M. (2017). The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives. *Masaryk University Journal of Law and Technology , 11*(1), 103-127.

Oun, M. A., & Bach, C. (2014). Qualitative Research Method Summary. *Journal of Multidisciplinary Engineering Science and Technology, 1*(5), 252-258.

Owsley, B. L. (2017). Network Investigative Source Code and Due Process . *Digital Evidence and Electronic Signature Law Review, 14*, 39-46.

Pawlaszczyk, D. (2022). Mobile Forensics – The End of a Golden Age? *Journal of Forensic Sciences and Criminal Investigation, 15*(4).

Penney, J., & Schneier, B. (2022). Platforms, Encryption, and the CFAA: The Case of WhatsApp v NSO Group. *Berkeley Technology Law Journal, 36*(101).

Perlroth, N., & Shane, S. (2019, May 25). In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc. *The New York Times*. Retrieved July 30, 2022, from https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

Peterson, A. (2015, May 28). U.N. Report: Encryption Is Important to Human Rights - and Backdoors Undermine It. *The Washington Post*. Retrieved July 30, 2022, from https://www.washingtonpost.com/news/the-switch/wp/2015/05/28/un-report-encryption-is-important-to-human-rights-and-backdoors-undermine-it/

Pfefferkorn, R. (2018). *Security Risks of Government Hacking.* The Center for Internet and Society (CIS). Retrieved July 30, 2022, from https://cyberlaw.stanford.edu/sites/default/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf

Pfefferkorn, R. (2021, December 14). We Now Know What Information the FBI Can Obtain from Encrypted Messaging Apps. *Just Security*. Retrieved from https://www.justsecurity.org/79549/we-now-know-what-information-the-fbi-can-obtain-from-encrypted-messaging-apps/

Pisaric, M. (2022). Communications Encryption as an Investigative Obstacle. *Journal of Criminology and Criminal Law (JCCL), 60*(1), 61-74.

Pool, R., & Custers, B. (2017). The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime. *The European Journal of Crime, Criminal Law and Criminal Justice, 25*(2), 123-144.

Poplin, C. M. (2016, April 13). Burr-Feinstein Encryption Legislation Officially Released. *The Lawfare Institute*. Retrieved July 30, 2022, from https://www.lawfareblog.com/burr-feinstein-encryption-legislation-officially-released

Priester, B. J. (2019). A Warrant Requirement Resurgence? The Fourth Amendment in the Roberts Court. *St. John's Law Review, 93*.

Privacy International. (2018). *Government Hacking and Surveillance: 10 Necessary Safeguards.* London: Privacy International. Retrieved July 30, 2022, from https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf

Propp, K. (2022). Has the Time for an EU-U.S. Agreement on E-Evidence Come and Gone? *Lawfare*. Retrieved July 30, 2022, from https://www.lawfareblog.com/has-time-eu-us-agreement-e-evidence-come-and-gone

Quattrocolo, S. (2020). Hacking by Law-Enforcement: Investigating with the Help of Computational Models and AI Methods. In *Artificial Intelligence, Computational Modelling and Criminal Proceedings* (pp. 37–71). Cham: Springer.

Radhakrishnan, K., Menon, R., & Nath, H. (2019). A Survey of Zero-Day Malware Attacks and Its Detection Methodology. *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, 533-539.

Reedy, P. (2020). Interpol Review of Digital Evidence 2016 - 2019. *Forensic Science International: Synergy, 2*, 489-520.

Reedy, P. (2021). The Risks for Digital Evidence. *Strategic Leadership in Digital Evidence*, 71-74.

Resecurity. (2021). *Cybercriminals Are Targeting Law Enforcement Agencies Worldwide.* Los Angeles: Resecurity, Inc. Retrieved July 30, 2022, from https://resecurity.com/blog/article/cybercriminals-are-targeting-law-enforcement-agencies-worldwide

Richards, P. J. (2017, April 18). *WIRED*. Retrieved July 30, 2022, from https://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers

Rivest, R. L. (1998). The Case against Regulating Encryption Technology. *Scientific American*, 116-117.

Roberts, G. (2022, July 31). Crime Boss Caged for 'Flooding' Bucks Town With Drugs. *Bucks Free Press, Crime & Court Reporter*. Retrieved August 1, 2022, from https://www.bucksfreepress.co.uk/news/20590814.crime-boss-caged-flooding-bucks-town-drugs/

Rojszczak, M. (2021). The Uncertain Future of Data Retention Laws in the EU: Is a Legislative Reset Possible? *Computer Law & Security Review, 41*.

Ropek, L. (2022, July 14). Ex-CIA Employee Convicted of Leaking 'Vault 7' Secrets to Wikileaks. *Gizmodo*. Retrieved July 30, 2022, from https://gizmodo.com/joshua-schulte-convicted-leaking-cia-vault-7-wikileaks-1849175952

Rozenshtein, A. Z. (2019, November 5). The WhatsApp-NSO Group Lawsuit and the Limits of Lawful Hacking. *The Lawfare Institute*. Retrieved July 30, 2022, from https://www.lawfareblog.com/whatsapp-nso-group-lawsuit-and-limits-lawful-hacking

Russell, Z. (2017). First They Came for the Child Pornographers: The FBI's International Search Warrant to Hack the Dark Web. *St. Mary's Law Journal, 49*(1), 269-[ii].

Salkind, N. J. (2012). *Exploring Research* (8th ed.). Pearson Education.

SANS. (2022). *FOR509: Enterprise Cloud Forensics and Incident Response*. (S. Institute, Producer) Retrieved July 30, 2022, from https://www.sans.org/cyber-security-courses/enterprise-cloud-forensics-incident-response/

Savage, S. (2018). Lawful Device Access Without Mass Surveillance Risk: a Technical Design Discussion. *CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 1761-1774.

Sawant, A. (2018). A Comparative Study of Different Intrusion Prevention Systems. *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 1-5.

Schaake, M., Pupillo, L., Ferreira, A., & Varisco, G. (2018). *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges.* Brussels: Centre for European Policy Studies (CEPS). Retrieved July 30, 2022, from https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press .

Schneier, B. (2015, July 30). Back Doors Won't Solve Comey's Going Dark Problem. *The Lawfare Institute*. Retrieved July 30, 2022, from https://www.lawfareblog.com/back-doors-wont-solve-comeys-going-dark-problem

Schneier, B. (2016). The Value of Encryption. *The Ripon Forum, 50*(2). Retrieved July 30, 2022

Schneier, B. (2018). *Security Risks of Government Hacking.* Schneier on Security. Retrieved July 30, 2022, from https://www.schneier.com/blog/archives/2018/09/security_risks_14.html

Servida, F., & Casey, E. (2018). IoT Forensic Challenges and Opportunities for Digital Traces. *Digital Investigation, 28, Supplement*, S22-S29.

Skorvanek, I., Koops, B.-J., Newell, B. C., & Roberts, A. (2019). 'My Computer Is My Castle': New Privacy Frameworks to Regulate Police Hacking. *Brigham Young University Law Review*(4), 997-1082.

Skrypnyk, A., & Titko, I. (2019). Use of Information from Electronic Media in Criminal Proceeding of Several European States: Comparative Legal Research. *Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law, 3*(15), 8-21.

Small, D. (2006). *New Code of Professional Standards for the Police.* Police Professional. Retrieved July 30, 2022, from https://www.policeprofessional.com/news/new-code-of-professional-standards-for-the-police/

Snyder, H. (2019). Literature Review as a Research Methodology: an Overview and Guidelines. *Journal of Business Research, 104*, 333-339.

Sommer, P. (2022). Evidence From Hacking: a Few Tiresome Problems. *Forensic Science International: Digital Investigation, 40*.

Srivastava , P., & Choudhary, A. (2021). Evolving Evidence Gathering Process: Cloud Forensics. In S. Tiwari, E. Suryani, A. K. Ng, K. Mishra, & N. Singh (Eds.), *Proceedings of*

International Conference on Big Data, Machine Learning and their Applications. Lecture Notes in Networks and Systems (Vol. 150). Singapore: Springer.

Stacho, P. (2022). *Navigating Trademark and Copyright Law in Cybersecurity.* ThriveDX. Retrieved September 22, 2022, from https://thrivedx.com/resources/article/navigating-trademark-law-in-cyber-security-awareness-training

Stanger, J. (2020). *The Ancient Practice of Steganography: What Is It, How Is It Used and Why Do Cybersecurity Pros Need to Understand It.* CompTIA. Retrieved July 30, 2022, from https://www.comptia.org/blog/what-is-steganography

Stepanovich, A., Bedoya-Arroyo, D., Bjorksten, G., Carbone, M., Mitnick, D., Wentworth, D., & White, N. (2016). *A Human Rights Response to Government Hacking.* Access Now. Retrieved July 30, 2022, from https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Communications Surveys & Tutorials, 22*(2), 1191-1221.

Stoykova, R. (2021). The Presumption of Innocence as a Source for Universal Rules on Digital Evidence. *Computer Law Review International, 22*(3), 74-82.

Swire, P. (2017). The Non-Code Aspects of Cybersecurity and the Globalization of Criminal Evidence. Georgia Institute of Technology, Institute for Information Security & Privacy. Retrieved July 30, 2022, from http://hdl.handle.net/1853/58843

Swire, P., & Ahmad, K. (2011). *'Going Dark' Versus a 'Golden Age for Surveillance'.* Center for Democracy and Technology. Retrieved July 30, 2022

Swire, P., Hemmings, J. D., & Vergnollie, S. (2016). A Mutual Legal Assistance Case Study: The United States and France. *Wisconsin International Law Journal, 34*(2), 323-366.

Syed, S., & Anu, V. (2021). Digital Evidence Data Collection: Cloud Challenges. *2021 IEEE International Conference on Big Data (Big Data)*, 6032-6034.

Tan, C., Zhang, L., & Bao, L. (2020). A Deep Exploration of BitLocker Encryption and Security Analysis. *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, 1070-1074.

T-CY Cloud Evidence Group. (2016). *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY.* Strasbourg: Council of Europe (CoE), Cybercrime Convention Committee (T-CY), Cloud Evidence Group. Retrieved July 30, 2022, from http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e

T-CY Cloud Evidence Group. (2016a). *Criminal Justice Access to Data in the Cloud: Cooperation with "Foreign" Service Providers.* Strasbourg: Council of Europe (CoE), Cybercrime Convention Committee (T-CY), Cloud Evidence Group. Retrieved July 2016, 2022, from http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d

Thompson, A. W. (2021, January 13). Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter. *Lawfare*. Retrieved July 30, 2022, from https://www.lawfareblog.com/assessing-vulnerabilities-equities-process-three-years-after-vep-charter

Tinoco-Pastrana, Á. (2020). The Proposal on Electronic Evidence in the European Union. *eucrim, Max Planck Institute for the Study of Crime, Security and Law*(1), 46-50. Retrieved from https://eucrim.eu/articles/proposal-electronic-evidence-european-union-spain/

Tosza, S. (2021). Internet Service Providers as Law Enforcers and Adjudicators. A Public Role of Private Actors. *Computer Law & Security Review, 43*.

Trummer, I. (2020). You Have the Right to Remain Silent; Anything You Say Will Be Gathered and Retained by the Government. *Tulane Journal of International and Comparative Law, 28*(2), 383-396.

Tung, L. (2016, March 2). France Could Fine Apple $1m for Each iPhone it Fails to Unlock. *ZDNet*. Retrieved July 30, 2022, from https://www.zdnet.com/article/france-could-fine-apple-1m-for-each-iphone-it-fails-to-unlock/

Twitter. (2022). *Guidelines for Law Enforcement.* Retrieved July 30, 2022, from https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support

UNODC. (2019). *Basic Tips for Investigators and Prosecutors for Requesting Electronic/Digital Data/Evidence from Foreign Jurisdictions.* Global Programme for Strengthening the Capacities of Member States to Prevent and Combat Serious and Organized Crime (GPTOC - GLOT32). The United Nations Office on Drugs and Crime. Retrieved July 30, 2022, from http://www.unodc.org/documents/legal-tools/Tip_electronic_evidence_final_Eng_logo.pdf

UNODC. (2019, June 20). *Informal International Cooperation Mechanisms*. Retrieved July 30, 2022, from United Nations Office on Drugs and Crime (UNODC):

https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/informal-international-cooperation-mechanisms.html

UNODC. (2021). *Data Disclosure Framework (DFF), General practices developed by international service providers in responding to overseas government requests for data.* Viena: The United Nations Office on Drugs and Crime (UNODC). Retrieved July 30, 2022, from https://sherloc.unodc.org/cld/uploads/pdf/El%20Evidence%20Hub/Data_Disclosure_Framework.pdf

US Secret Service. (2015). *Best Practices For Seizing Electronic Evidence - Version 4.2.* The US Secret Service. The US Department of Homeland Security. Retrieved July 30, 2022

Valentino-DeVries, J. (2019, April 13). Tracking Phones, Google Is a Dragnet for the Police. *The New York Times*. Retrieved from https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

Veen, J., & Boeke, S. (2020). No Backdoors: Investigating the Dutch Standpoint on Encryption. *Policy & Internet, 14*(4), 503-524.

Verdelho, P. (2019). Obtaining Digital Evidence in the Global World. *EU Law Journal, 5*(2), 136-145.

Vermeer, M. J., Woods, D., & Jackson, B. (2018). *Identifying Law Enforcement Needs for Access to Digital Evidence in Remote Data Centers.* Santa Monica: RAND Corporation. Retrieved July 30, 2022, from https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2240/RAND_RR2240.pdf

Vodafone. (2021). *Country by Country Disclosure of Law Enfrocement Assistance Demand.* Vodafone Group Plc. Retrieved from https://www.vodafone.com/sites/default/files/2021-02/Vodafone_LED_country_by_country_2019-20_AW4_V4.pdf

Walden, I. (2018). 'The Sky is Falling!' – Responses to the 'Going Dark' problem. *Computer Law & Security Review, 34*(4), 901-907.

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access, 8*, 85094-85115.

Wani, M. A., AlZahrani, A., & Bhat, W. A. (2020). File System Anti-Forensics – Types, Techniques and Tools. *Computer Fraud & Security, 3*, 14-19.

Welty, J. (2018, July 23). Search Warrants Authorizing Law Enforcement Computer Hacking and Malware. *North Carolina Criminal Law*. Retrieved July 30, 2022, from https://nccriminallaw.sog.unc.edu/search-warrants-authorizing-law-enforcement-computer-hacking-and-malware/

Wilkinson, S. (1998). Focus Group Methodology: a Review. *International Journal of Social Research Methodology, 1*(3), 181-203.

Wilson, N., Sheldon, A., Dries, H., Schafer, B., & Mason, S. (2021). Proof: the Technical Collection and Examination of Electronic Evidence. In S. Mason, & D. Seng (Eds.), *Electronic Evidence and Eloctronic Signatures* (Fifth ed., pp. 429-487). London: Institute of Advanced Legal Studies.

Wise, P., & Mount, I. (2022, May 10). Spain's intelligence chief sacked over Pegasus spyware crisis. *Financial Times*. Retrieved from https://www.ft.com/content/3222f298-e1da-4538-a7a3-32ad394e8227

Working Party. (2018). *Article 29 WP Statement on encryption (ePrivacy).* Article 29 Data Protection Working Party. Retrieved July 30, 2022, from https://ec.europa.eu/newsroom/article29/redirection/document/51026

Yadav, R., Verma, R., & Solanki, A. (2019). Defense-in-Depth Approach for Early Detection of High-Potential Advanced Persistent Attacks. In K. Ray, T. Sharma, S. Rawat, R. Saini, & A. Bandyopadhyay (Eds.), *Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing* (Vol. 742). Singapore: Springer.

Yaqoob, I., Hashem, I. A., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2019). Internet of Things forensics: Recent Advances, Taxonomy, Requirements, and Open Challenges. *Future Generation Computer Systems, 92*, 265-275.

Yin, R. K. (2003). *Case Study Research: Design and Methods* (3rd ed.). SAGE.

Zagaris, B., & Plachta, M. (2020). Transnational Organized Crime. *International Enforcement Law Reporter, 36*(7), 248-255.